METODOLOGÍA PARA LA APLICACIÓN DE PROTOCOLOS DE SEGURIDAD EN PLATAFORMAS INDUSTRIALES DESACTUALIZADAS BAJO LAS NORMATIVAS IEC 61508 E IEC 61511

Carlos Ariel García Montoya

Proyecto de grado presentado como requisito parcial
para aspirar al título de Magister en Ingeniería Eléctrica

Director
Mauricio Holguín Londoño, Ing. M.Sc, Ph.D

Co-director
Germán Andrés Holguín Londoño, M.Sc, Ph.D(C)

UNIVERSIDAD TECNOLÓGICA DE PEREIRA
PROGRAMA DE MAESTRÍA EN INGENIERÍA ELÉCTRICA
PEREIRA
2021

Nota de Aceptación

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma de jurado 1 - Evaluador

_____

Firma del jurado 2 - Evaluador

_____

Firma del jurado 3 - Director

Dedicado a mis abuelas Luisa, María, Laura y Lola, a mis abuelos Carlos y Enrique a mi madre Mercedes y a mi padre Ariel.

Agradecimientos...

A mi tutor, el Ing. Mauricio Holguín Londoño por todo el apoyo profesional y personal que me ha brindado en mi paso por la UTP.

A mis familiares, amigos y compañeros de trabajo que me han apoyado y alentado para el crecimiento académico día a día.

A mi esposa Alejandra, a mis hijos Yesid, Alejandro y Santiago quienes han vivido cada paso de este proceso con humildad, cariño y compresión.

CONTENIDO

pág.

LISTA DE FIGURAS

LISTA DE TABLAS

1. PLANTEAMIENTO DEL PROBLEMA

Un importante sector de la industria nacional cuenta con una plataforma industrial antigua, la cual tiene un desplazamiento frente a las nuevas tecnologías por obsolescencia, deficiencia productiva y estándares de seguridad desactualizados, motivos que incentivan un cambio de equipos o una renovación de estos [3] [4].

La opción de reemplazo de maquinaria presenta altos costos y paros largos en líneas de producción, lo que hace más viable realizar una actualización tecnológica en el control de manufactura y de seguridad de las líneas de fabricación, que mejore la producción reduciendo los desperdicios y la accidentalidad [4].

Los diseños de máquinas desactualizadas están enfocados hacia la parte física de esta, no monitorean los valores y parámetros de operación dentro de límites de funcionamiento, no generan alarmas ni conducen la planta a condiciones seguras después de una parada de emergencia, la acción de control más frecuente en su programación es simplemente la desconexión. Estos controles se fundamentaban, inicialmente, en sistemas de relevación electromecánicos y posteriormente evolucionaron a controles por PLC (controladores lógicos programables). Paralelamente, las normativas de seguridad también evolucionaron desde los inicios de la industria, donde los accidentes eran normales y tolerables, hasta hoy en día donde la seguridad prima sobre los aspectos productivos y se apoyan en las reglamentaciones internacionales como la OSHA en Estados Unidos de América, las reglamentaciones de la comunidad Europea y las normativas IEC (Internacional Electrotechnical Commission) como la 61508 y 61511 [3] [5].

La evolución de los sistemas de control de seguridad ha permitido la continua mejora en los puestos de trabajo, partiendo desde los inicios con elementos de corte de energía electromecánicos, pasando a las lógicas de control por relés de contacto seco, hasta la llegada de los PLC, en los cuales se realiza el control del proceso y la seguridad de

este. En la actualidad, se hace indispensable el tener los PLC de seguridad dedicados, dada la importancia actual de la seguridad para el personal operativo y para el proceso de producción, o el diseño de sistemas de seguridad que respeten los estándares, pero existe el inconveniente de poder describir y evaluar de forma adecuada los niveles de seguridad exigidos en cada tipo de industria [3] [4] [5].

Las funciones de seguridad no se deben mezclar con el control del proceso, como tampoco ser manipulables por los usuarios finales, ya que perderían credibilidad, confiabilidad y funcionabilidad; estos aspectos son clave en un sistema que supervisa la operación de un proceso [4] [5]. En la actualidad, las líneas de manufactura deben contener las herramientas necesarias para minimizar la exposición y el riesgo del personal humano y tener condiciones seguras de trabajo, siendo estas una necesidad de obligatorio cumplimiento para las empresas. Estas herramientas son enlazadas con el sistema de seguridad diseñado para vigilar que se cumplan los procesos bajo el marco de las normativas de seguridad internacionales, pero actualizar estas líneas a los estándares modernos presentan diferentes dificultades como son: altos costos, modificaciones mayores inviables, sistemas de control cerrados de exclusividad de fabricante, o simplemente no son actualizables.

En [6] se analizó el artículo titulado "Fuera de control" (Out of Control), estudio de La Autoridad Británica Health and Safety Executive - HSE, publicado en el año 1995, donde se explora que el origen de las causas de varios accidentes industriales fue por fallas en los equipos de control y se concluyó lo siguiente: 44 % de los accidentes se debieron a deficiencias en las especificaciones de los equipos e instrumentos; 15 % a deficiencias en el diseño e instalación; 6 % ocurrió durante el arranque de la planta; 15 % fue durante el mantenimiento y operación y 20 % se debió a cambios y modificaciones después del arranque de la planta. El resultado de este estudio es lo que llevó al desarrollo de "el ciclo de vida" de seguridad funcional y a implementar las normas internacionales

de seguridad funcional tales como: la ISA S84.01 de 1996, la IEC 61508 de 1998 y la IEC 61511 del año 2003.

Por otro lado, los tratados comerciales, las legislaciones locales e internacionales obligan a la actualización de los sistemas de seguridad en máquinas de producción y transformación de materiales [7]; estos cumplimientos son reflejados en la disminución del número de accidentes laborales, en la identificación y reducción de procesos inseguros y en la disminución de enfermedades profesionales por exposición, reduciendo cada vez más la probabilidad de lesiones por causa del trabajo.

Por lo tanto, se genera la necesidad de realizar una metodología para la aplicación de las normativas especializadas en seguridad de máquinas en procesos industriales con estándares de producción de alta calidad [4] [5] [8]. Las normas de seguridad actuales para la industria de proceso están basadas en la IEC 61508 y la IEC 61511, las cuales se enfocan en la reducción del riesgo y en el establecimiento de un óptimo grado operacional en cada ciclo de vida del proyecto de seguridad [1].

Con el presente proyecto de grado, se busca indagar si es posible aplicar los estándares de seguridad en máquinas de procesos industriales no conformes bajo los estándares de seguridad indicados en las normas IEC 61508 e IEC 61511, donde se ajusten los protocolos y funcionalidades actuales, según el número de operaciones y maniobras demandadas por el proceso.

2. JUSTIFICACIÓN

Las máquinas de la industria de manufactura deben cumplir las normas vigentes para garantizar la seguridad y reducir los riesgos en el factor humano. En la aplicación de los sistemas de seguridad actuales se emplean las normas de sistemas de seguridad IEC 61508 e IEC 61511; los sistemas de producción con carencias en los aspectos de seguridad se consideran obsoletos [9] [8], lo que hace necesario actualizar los equipos en la industria, reemplazando los sistemas de control en especial los relacionados con la seguridad.

Debido a esto, se debe desarrollar una metodología para actualizar los protocolos de seguridad en las plataformas industriales desactualizadas, bajo las normativas IEC 61508 e IEC 61511, generando un ciclo de vida para la plataforma a utilizar en la cual se establezca el nivel de integridad de la seguridad, basándose en un SIS (Sistema Integrado de Seguridad), que contemple elementos físicos (hardware HW) y los elementos de programación (software SW) [8] [10]. Para el caso de la industria de manufactura, el proceso después de establecer el SIL (Safety Integrity Level - nivel de integridad del sistema de seguridad) requerido, es plantear el reemplazo de los elementos del sistema de seguridad que no cumplan con el nivel de SIL requerido. Alcanzando el nivel de integridad de la seguridad (SIL 1, 2 ,3 para las máquinas de manufactura) [11], el proceso puede certificarse dentro de los marcos de producción segura requeridos en las normatividades internacionales para la comercialización y/o para la viabilidad de su operación.

Aplicar protocolos para actualizar las plataformas de producción es pertinente, ya que los continuos cambios tecnológicos y los desarrollos en el campo de la seguridad y salud laboral se han convertido en una oportunidad de mejora en los puestos de trabajo, en la reducción de accidentalidad, tiempo perdido y ausentismo laboral, reduciendo

y/o eliminando los costos asociados a estos factores e impactando positivamente las compañías en términos de un lugar más seguro para trabajar, valor esencial en los procesos de manufactura del siglo XXI [7].

La viabilidad está marcada por la necesidad de actualización de las plataformas de producción funcionales actualmente en la industria, por ejemplo, en las máquinas papeleras, maximizando la rentabilidad desde el aspecto productivo y con los criterios de seguridad de los procesos actuales. Estas máquinas son muy valiosas y su reemplazo por líneas nuevas no son plenamente justificables, pero las actualizaciones son una buena alternativa en la relación costo beneficio [11].

Los modelamientos de los sistemas de seguridad se han realizado por diferentes métodos como son, cálculos por redes de confiabilidad y árboles de confiabilidad, entre otros [8] [12], que se han logrado implementar en los sistemas nuevos [13]. Como el desarrollo de este proyecto es para aplicar en un modelo desactualizado, no se logra acoplar estos métodos ya que sus ecuaciones son rígidas y pensadas para las nuevas tecnologías de seguridad con sistemas modernos. Para el caso de sistemas desactualizados, una adecuada solución son las cadenas de Markov, como en [6], ya que es un método muy común para modelar estadísticamente procesos aleatorios. Las cadenas de Markov permiten analizar los diferentes modos de falla, además las normas IEC [14] [15] [16] recomiendan su uso para el cálculo del PFDavg (Probabilidad promedio de falla bajo demanda), y el PFH (frecuencia promedio de fallas peligrosas por hora) entre otros que dan un indicador de la fiabilidad del sistema.

En la actualidad, gran parte de industria nacional tiene plataformas de producción con alta antigüedad, estas representan una fuente importante de mano de obra, dado que requieren mayor personal para su operación frente a las máquinas más modernas y automatizadas, pero a su vez son máquinas que generan mayor riesgo operativo, por lo tanto, la opción de actualizar estos procesos de manufactura en los aspectos de

seguridad aseguran la continuidad de las líneas de producción, de las empresas y las fuentes de empleo de manera segura [11].

Es por todo lo descrito que, con la elaboración del presente proyecto, se busca desarrollar una metodología para aplicación y guía en los procesos de actualización de seguridad en las líneas de manufactura con plataformas desactualizadas, bajo las normativas IEC 61508 e IEC 61511 y aplicando las cadenas de Markov como medio para describir y analizar los nuevos requerimientos en seguridad.

3. OBJETIVOS

3.1. Objetivo General

Desarrollar una metodología para adaptar las condiciones de operación segura, con base en funciones y sistemas instrumentados de seguridad, en sistemas con plataformas desactualizadas, de acuerdo con las normativas IEC 61508 y 61511, y aplicando las cadenas de Markov como medio para describir y analizar los nuevos requerimientos en seguridad.

3.2. Objetivos Específicos

1. Indagar los requerimientos contenidos en las normas IEC 61508 e IEC 61511 en cuanto a las demandas de seguridad en los procesos

2. Establecer las configuraciones que permiten llegar a alcanzar un nivel de conformidad con los requerimientos de norma, según un nivel de integridad de seguridad demandado.

3. Desarrollar una metodología para adaptar los requerimientos de SIL por norma con funciones y sistemas instrumentados de seguridad para aplicación en plataformas no conformes, empleando cadenas de Markov.

4. Aplicar y validar la metodología desarrollada a un sistema industrial con plataforma no conforme.

4. MARCO TEÓRICO Y CONCEPTUAL

4.1. Estado del arte

La evolución de los sistemas de control de seguridad ha permitido la continua mejora en los puestos de trabajo. Partiendo desde los inicios, en el año de 1975 se disponía para los diferentes controles industriales con tecnologías de relés y electrónica de estado sólido, pero en ellas simplemente la seguridad no se podía concebir, posteriormente con la llegada de los PLC de control en 1980, en los cuales se realiza el control del proceso, se presentaban problemas de relevación electromecánica, fallas en los dispositivos de entrada y salida sin ningún tipo de seguridad.

Hacia el año de 1984, se generan las primeras normativas TÜV, Orientadas hacia Tecnología de Microprocesadores; en 1985 se implementan los primeros sistemas redundantes triples, para posteriormente en 1986 iniciar con los primeros diseños de PLC de seguridad. En 1989 se publican las normas alemanas DIN 19250 / VDE 0801, las cuales se orientaban hacia las aplicaciones, considerando principalmente resoluciones lógicas [12].

Durante muchos años, los sistemas de seguridad fueron proyectados según las normas alemanas, donde estas se referirían a lo relacionado con la evaluación de riesgos (DIN V 19250), los requisitos generales para dispositivos de protección (DIN V 19251) y computadoras en sistemas con tareas de seguridad (DIN V VDE 0801) [17].

Posteriormente, estas normas se integraron a las normas europeas, las cuales fueron bien aceptadas por mucho tiempo. En 1994 aparece la norma VDE 0801: Armonización con Estándares Internacionales Emergentes. Dado los reportes de varios accidentes mayores a nivel mundial, los expertos en seguridad en la industria de procesos revisaron las normas de seguridad existentes, entre sus conclusiones estaba que las normas eran

demasiado específicas a la industria y limitaban la habilidad de los expertos en seguridad de compartir las mejores prácticas. A partir de esto, se conformó el comité ISA SP84, el cual que dio un enfoque más adecuado a las normas, usando un modelo que se denominó Ciclo de Vida de Seguridad, aproximación Cuantitativa, en 1996 [18] [12] [16] [10] [17].

Finalmente se llegó a conformar en 1997 una norma IEC que consideraba el lazo completo, ciclo de vida de seguridad, aproximación cualitativa y cuantitativa. En el año 1998, fue emitida la norma con requisitos básicos, con acreditación internacional a través de la Comisión Electrotécnica Internacional (International Electrotechnical Commission, IEC). Esta norma es la que hoy se conoce como la IEC 61508 "Seguridad Funcional de los Sistemas Eléctricos, Electrónicos, Electrónicos Programables relacionados a la Seguridad". A partir de esta norma base, se heredaron una serie de normas de aplicación para diferentes industrias de procesos (industria petroquímica, pulpa y papel, industria textil entre otras), en las que se definieron los requisitos organizacionales y técnicos exigidos a las instalaciones de seguridad, y a su implementación. El estándar internacional IEC 61508 intenta potencializar la mejoría de los PES (Programmable Electronic Safety), que abarcan los PLC, los sistemas de control distribuido, sensores y actuadores inteligentes, entre otros, alineando los conceptos involucrados. Además, ha sido altamente aceptada como base para la especificación, diseño y operación de los Sistemas Instrumentados de Seguridad (SIS) [19] [14].

Esta norma fue usada por algunas plantas de procesos, pero al ser una norma tan general para la industria, rápidamente se dieron cuenta que requerían heredar otras normas más específicas a las diferentes ramas de la industria [20], por ello en 2004 se aprobó la norma IEC 61511, denominada "Seguridad funcional: SIS para el sector de la industria de proceso", la cual es una norma de aplicaciones unificada para la industria de procesos [19] [15]. Esta última norma aplica tanto a fabricantes como a integradores y usuarios finales, contiene los requerimientos para el diseño y gestión

del Sistema Instrumentado de Seguridad (SIS) a lo largo del todo el ciclo de vida de la seguridad, su alcance incluye: concepto inicial, diseño, implementación, operación, mantenimiento y desmantelamiento [15].

Los sectores de la industria que abarca esta norma son: petróleo y gas, química, energía, farmacéutica y pulpa y papel; por ello la norma IEC 61511 cubre el uso de equipos eléctricos, electrónicos y electrónicos programables, también es aplicable a los equipos que utilizan sistemas hidráulicos o neumáticos para maniobra final, pero no cubre el diseño o implementación de la lógica neumática o hidráulica [21].

4.2. Ciclo de vida de seguridad

La primera parte de la norma IEC 61508 analiza el ciclo de vida completo de la seguridad, con requisitos detallados en cuanto al procedimiento y contenido de los distintos pasos. Esta parte tiene una importancia fundamental para fabricantes de máquinas y de componentes de seguridad.

En la figura1 se visualiza el ciclo de vida de la seguridad (SIS), en el cual, cada elemento que la compone debe cumplir con este paso a paso y es de obligatorio cumplimiento para fabricantes, integradores y usuarios finales [1].

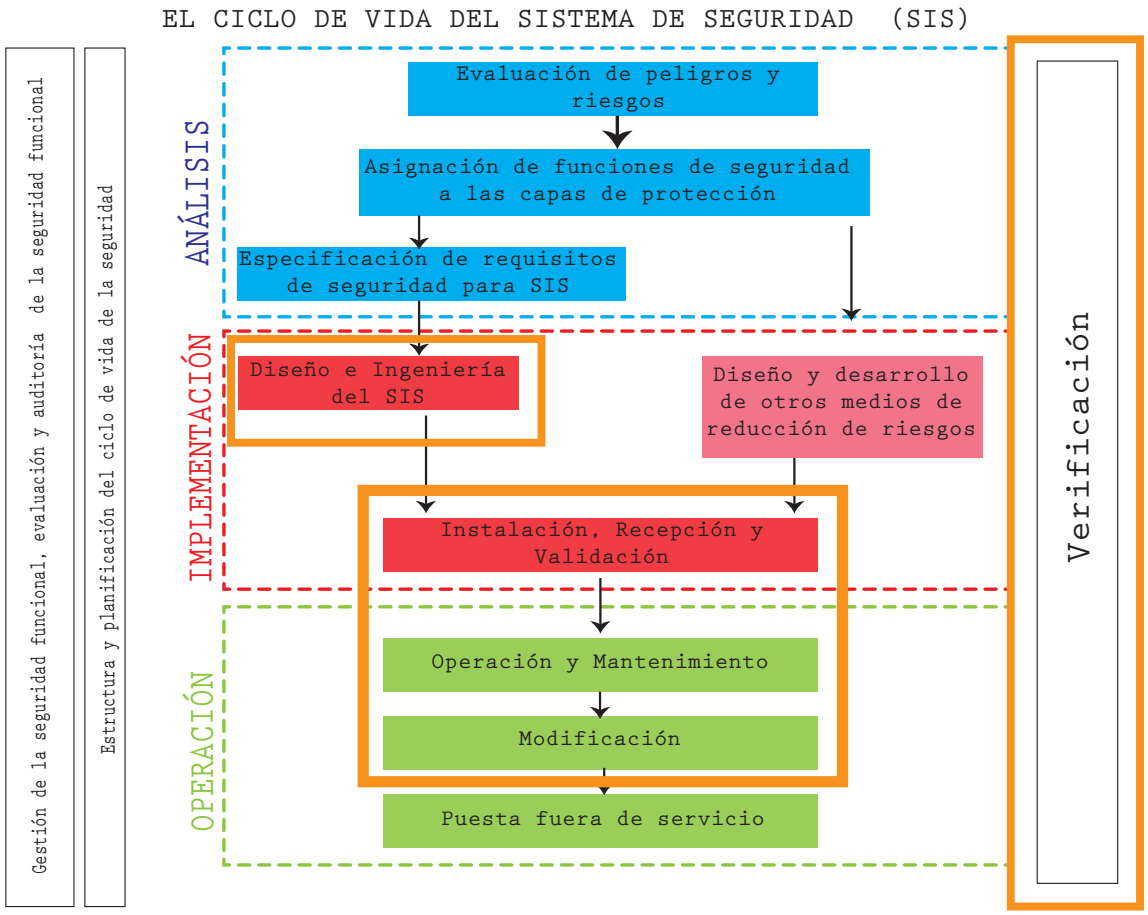


Figura 1. Ciclo de vida de la seguridad. Tomada de [1].

4.3. SIS Sistema Instrumentado de Seguridad

Un sistema instrumentado de seguridad puede ser definido como: "un sistema compuesto por sensores, lógica y elementos finales con el propósito de reducir los riesgos en los procesos y llevarlos a un estado seguro, cuando determinadas condiciones se cumplen", estos conforman las funciones de seguridad (SIF). Es, por tanto, crítico y fundamental que las empresas de proceso tengan en consideración en sus proyectos que la seguridad industrial de sus instalaciones pasa por el cumplimiento estricto de cada paso del ciclo de vida que definen y procedimentan los actuales estándares internacionales (ISO e

IEC) [10] [8].

4.4. SIL - Nivel de Integridad de la Seguridad

El término SIL se refiere al nivel de integridad de la seguridad, este hace referencia a la categoría que requiere un proceso y también hace referencia al nivel de desarrollo que tiene un elemento, está categorizado de 1 a 4 [22] [10]. En la industria de procesos se encuentra de 1 a 3 y el nivel SIL 4 está para desarrollos de tipo nuclear. En la industria nacional tenemos líneas de producción con diferentes zonas en las que se requieren desarrollos de seguridad con categorías SIL 1, 2, y 3 por ejemplo: en la industria papelera una línea de conversión puede presentar los diferentes niveles de seguridad así: zona de gofrado (SIL 3), rebobinado (SIL 3), des bobinado (SIL 2), alimentación de producto (SIL 1) y como este sector se tienen otros sectores de manufactura factibles de implementar los sistemas de seguridad.

4.5. PLC de seguridad

El PLC de seguridad es un elemento más avanzado al PLC tradicional, ya que cuenta con capacidad de diagnóstico de fallas en las señales de entrada y de salida. Para lograr esto, se han desarrollado diferentes arquitecturas en las entradas y las salidas, vigilando la funcionalidad del sistema de control y cumpliendo con un nivel de integridad determinado (SIL) de acuerdo con el proceso requerido [23] [24]. En la siguiente imagen (figura 2), se muestra gráficamente un ejemplo de las diferencias fundamentales entre un PLC estándar y un PLC de seguridad, para este caso el PLC estándar presenta una arquitectura 1oo1, mientras que el PLC de seguridad presenta una arquitectura 1oo2D [25].

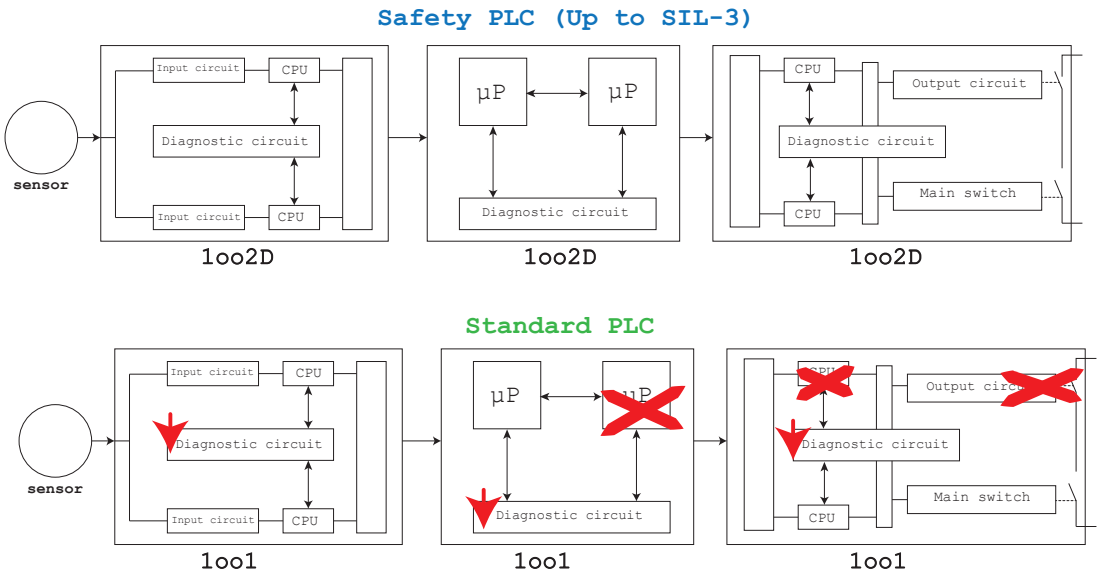


Figura 2. Diferencias entre PLC y PLC de seguridad. Tomada de [2].

La arquitectura 1oo1, es la tradicional entrada o salida de un PLC estándar, si se presenta un daño para el ingreso de la señal o para la salida de control, no se tiene la capacidad de detectar la anomalía, por lo cual se desarrollaron arquitecturas con capacidad de diagnóstico del estado de entrada o salida a evaluar.

Arquitectura 1oo2 (lógica 1 de 2) proporciona mayor nivel que la arquitectura 1oo1 ya que si un canal falla el otro puede operar el sistema de seguridad. Además, de estas 2 arquitecturas, se han desarrollado otras diferentes utilizadas en las plataformas de sistemas de seguridad [23] [26].

5. SEGURIDAD EN PROCESOS INDUSTRIALES

En la actualidad, entre mayor producción con calidad se genere en una empresa, mayor serán las utilidades de esta, por lo que un tema muy relevante es mantener en todo momento la fábrica en producción, con altos estándares de calidad y con procesos lo más seguros posibles. Ahora, el alto número de accidentes que se producen en los procesos industriales puede ser causado por el poco conocimiento e implementación existente sobre la seguridad de las máquinas. Por estas razones, es indispensable aplicar normativas como la IEC 61508 o la IEC 61511 con las cuales se indica cuán seguro es el proceso mediante un nivel de integridad de seguridad (SIL, Safety Integrety Levels) específico, que se implementa por medio de un sistema instrumentado de seguridad (SIS, Safety Instrumented System) a fin de alcanzar o mantener un estado seguro [27].

5.1. Función instrumentada de seguridad – Safety Instrumented Function (SIF)

Es una función diseñada para detectar una situación de riesgo y automáticamente tomar las medidas necesarias para prevenir o mitigar dicho suceso peligroso. Está compuesto por i) detectores o sensores, ii) solucionador de lógica como computador, PLC, etc., y por iii) accionadores, como válvulas, frenos, etc. [27] [28]. Una SIF, y sus partes, se pueden observar en la figura 3.

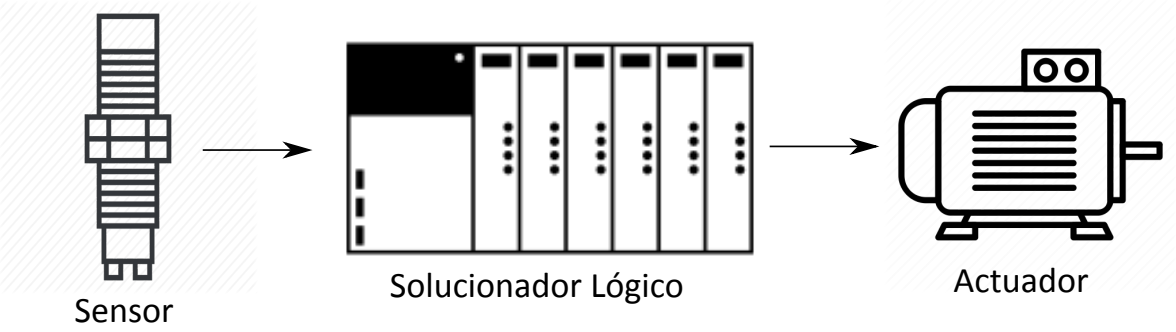


Figura 3. Función instrumentada de seguridad. Fuente el autor.

Para cada suceso de riesgo se realiza una Función Instrumentada de Seguridad (Safety Instrumented Function - SIF) la cual se diseña para detectar una situación de riesgo y, automáticamente, tomar las medidas necesarias para prevenir o mitigar dicho suceso peligroso. Cada función de seguridad recoge y analiza información de los sensores para determinar si esto produce una condición peligrosa y así, en consecuencia, se produce una secuencia de parada para poder llevar el proceso a un estado seguro [29] [30].

5.2. Sistemas Integrados de Seguridad – Safety Instrumented System (SIS)

Es un sistema que implementa las funciones de seguridad (SIF) requeridas y necesarias para lograr o mantener un estado seguro para algunos equipos. Este se utiliza frecuentemente para reducir los procesos peligrosos en plantas de producción [28] [27]. Un SIS puede constar de varios SIF, tal como se enseña en la figura 4.

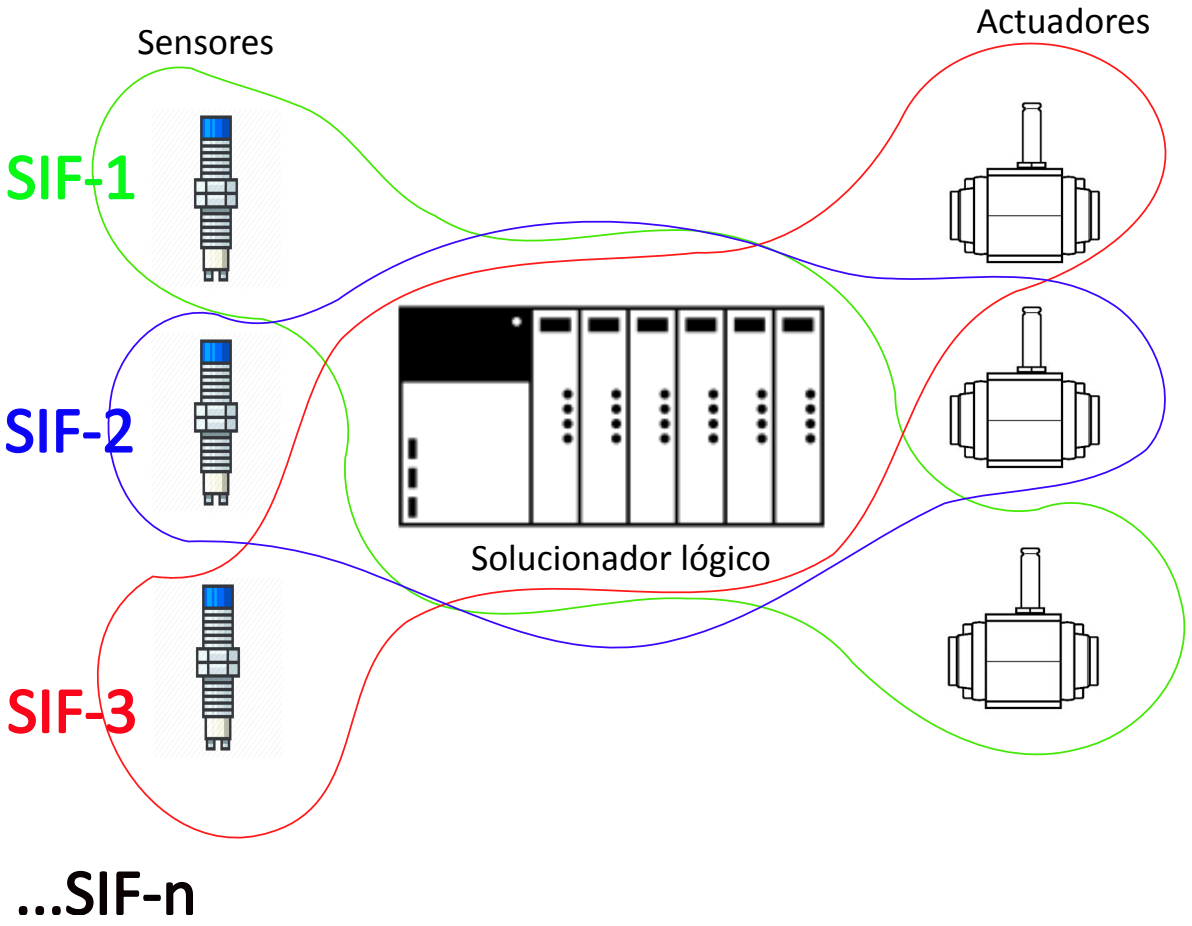


Figura 4. Sistema integrado de seguridad. Fuente el autor.

El diseño de una SIF depende del tipo de falla a tratar. Se distinguen dos tipos de fallas, a saber: una falla segura, en la cual se desea energizar la salida de la función de seguridad, pero al realizar la orden de activación esta no se activa generando que el actuador se mantenga inactivo; por otro lado, se puede tener una falla peligrosa, en la cual se desea desactivar la salida de la función de seguridad, sin embargo, al realizar la orden de desactivación esta no se desactiva generando que el actuador se mantenga activo [28] [30].

5.3. Nivel de prestación (PLr)

Se define como la capacidad de un sistema de mando para ejecutar la función de seguridad y con ello mitigar el riesgo deseado. Este nivel de PLr se divide en niveles de la "a" a la "e", donde "a" representa un nivel de fiabilidad bajo y "e" representa el nivel de fiabilidad más alto [31].

Para cada función de seguridad se hace necesario determinar el nivel de prestación requerido (PLr) o nivel de rendimiento, es decir la cantidad de reducción de riesgo que posee cada parte del sistema de mando, relativas a la seguridad. Entonces PLr es el valor deseado para la función de seguridad, mientras que PL es el resultado del análisis, o valor real obtenido.

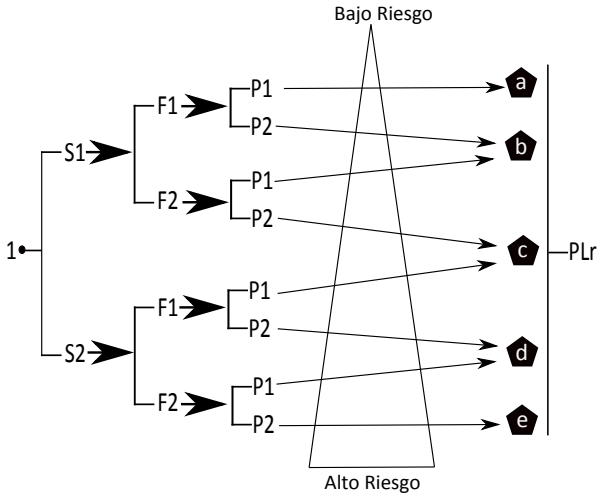


Figura 5. Nivel PL. Fuente el autor.

Para determinar los 5 niveles del PLr se tienen unos parámetros (S, F, P) para la selección del nivel demandado (ver figura 5). Estos parámetros se dividen en dos grupos:

Severidad del daño.

- S –Gravedad de la lesión

Probabilidad de ocurrencia.

- F – Frecuencia / tiempo exposición peligro
- P – Posibilidad de evitar o limitar el peligro

Los 5 niveles inician en la letra “a”, o con una contribución baja a la reducción de riesgo (indicado como L); y terminan en la letra “e”, o una contribución alta a la reducción de riesgo (indicado como H).

Para determinar el PLr se inicia con definir la severidad del daño (S), como se observa en la figura 6 [29], y dividido en los grupos S1 y S2, así:

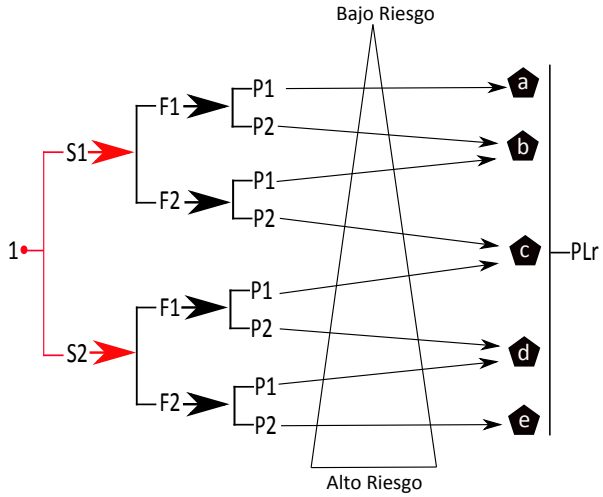


Figura 6. Gravedad de la lesión. Fuente el autor.

S1 – Leve (normalmente reversible): el fallo de la función de seguridad solo conlleva a daños leves. La persona afectada tras algún tratamiento médico queda en la misma situación que antes del daño. Es decir sólo se tienen daños leves como golpes, contusiones o heridas leves.

S2 – Grave (normalmente irreversible): el fallo de la función de seguridad conlleva habitualmente daños graves, irreversibles, es decir, la persona directamente afectada quedará con heridas que conllevan a secuelas permanentes o, en ocasiones, incluso la muerte.

Luego, para el PLr, se define la frecuencia (F) o tiempo de exposición peligroso, como se muestra en la figura 7, con los siguientes dos grupos:

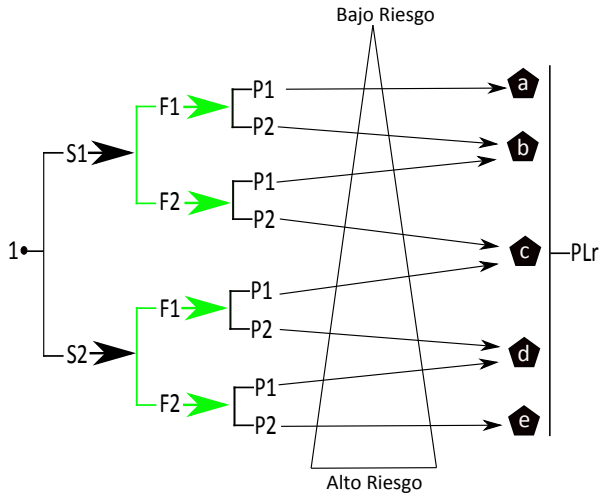


Figura 7. Frecuencia o tiempo de exposición al peligro. Fuente el autor.

F1 – De raramente a poco frecuente o tiempos cortos de exposición: se selecciona F1 únicamente en los casos donde sólo se tiene acceso ocasionalmente, sin mucho tiempo de duración.

F2 – De frecuente a continua o tiempos largos de exposición: se debe seleccionar F2 cuando se tiene acceso frecuentemente o de manera continua a la fuente de peligro, ya sean una o varias personas las expuestas al peligro o si se exponen de forma sucesiva, por ejemplo, en el caso de los ascensores. Si la frecuencia es superior a una vez por hora, se debe seleccionar F2 siempre que no exista otra justificación [29].

Finalmente, para el PLr, se define la posibilidad de evitar o limitar el peligro (P), como se indica en la figura 8:

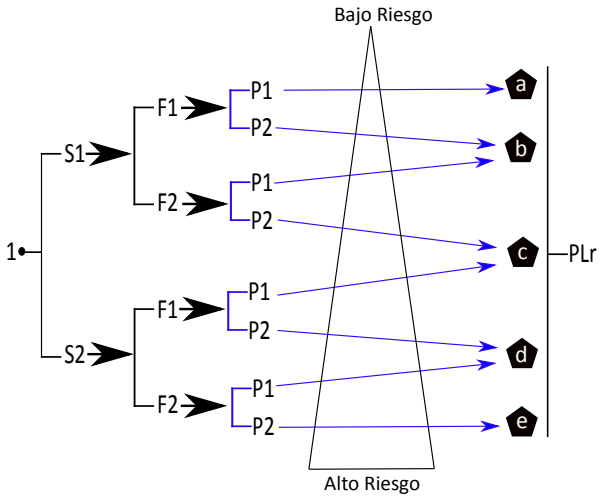


Figura 8. Posibilidad de evitar o limitar el peligro. Fuente el autor.

P1 – Posible bajo ciertas condiciones: si se tiene una posibilidad que sea realista de evitar o al menos reducir el peligro o accidente y sus efectos. **P2 – Raramente posible:** se selecciona en caso de presentarse una situación peligrosa o de accidente de forma casi segura, es decir cuando se presenta una alta probabilidad de daño, o poca probabilidad de evitarlo.

La selección del parámetro P1 ó P2 puede venir determinada por diferentes condicionantes, como:

- Si la identificación del peligro es directa o es necesaria la ayuda de instrumentos para detectarlo (por ejemplo, indicadores de niveles de presión o de contaminación).

- El tipo de operación, por ejemplo, si ésta se realiza con o sin supervisión, por personal experto o por no profesionales. Otro posible criterio es la existencia de métodos de trabajo seguros implementados.

- La velocidad de ocurrencia del peligro, sobre todo en relación con el tiempo de reacción del operario.

- La posibilidad de evitar el peligro cuando este se produzca, por ejemplo, si existen

vías de escape o mecanismos de emergencia efectivos cercanos a la zona de operación.

Ejemplo: "Parada segura de un husillo (tornillo sin fin) en el momento de abrir la cubierta de seguridad", en este caso, para calcular el PLr se procede como sigue:

- Determinar la importancia de los daños (S): para este caso, se tiene un nivel S2 donde se puede ocasionar una lesión grave (irreversible) y hasta la muerte.

- Determinar la frecuencia y/o el tiempo de exposición que se tiene al peligro (F): en este caso se tiene F2, debido a que se tiene una larga exposición y/o mayor frecuencia hasta permanente.

- Determinar la probabilidad de evitar el peligro o al menos minimizar los daños (P): es P1 ya que es posible evitar el riesgo en ciertas condiciones. Con estos datos, se puede utilizar el árbol de selección para el PLr, el cual queda de la manera indicada en la figura 9:

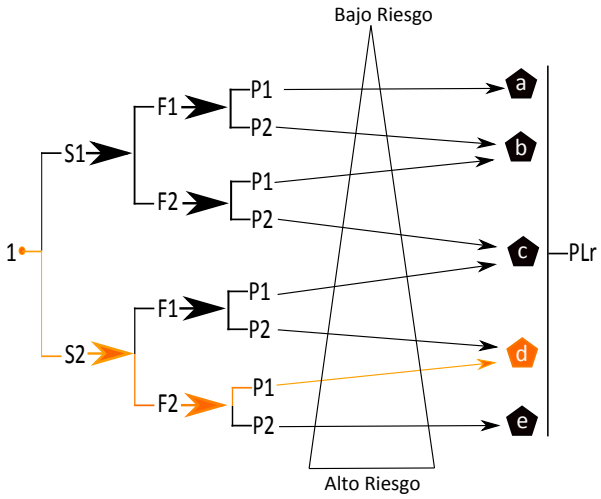


Figura 9. Ejemplo SFP. Fuente el autor.

De esta manera se puede observar que se obtiene un nivel PLr igual a "d", el cual sirve luego para la evaluación del riesgo y del PL obtenido, o real [29].

6. FALLOS DE CAUSA COMÚN Y COBERTURA

6.1. Fallos de causa común (CCF)

Las fallas de causa común son una seria amenaza para la confiabilidad de los SIS, ya que se pueden provocar fallas simultaneas de componentes. Según la norma IEC 61508, se define falla común como una falla que resulta en uno o más eventos causando fallas en varios canales, si el sistema es multicanal, lo cual da lugar a una falla en el sistema. Se define como un fallo no detectado.

Los CCF ocurren cuando se presenta un fallo peligroso ocasionado por múltiples fallos resultantes de una sola causa. Un ejemplo puede ser un cortocircuito.

En la norma EN IEC 62061 se puede encontrar la Tabla 1 para puntuar las medidas empleadas contra las CCF, esta puntuación se suma para determinar el factor de falla común (B).

Para la estimación de este parámetro, se tiene en cuenta que es un proceso cuantitativo que se debe realizar para todo el conjunto de sistemas de mando relativos a la seguridad, en el cual se debe establecer un método simplificado basado en un sistema de puntuación. Mediante una serie de medidas para reducir los fallos de causa común, las cuales poseen cada una su propia puntuación. Cuando se tienen estas medidas, se suman las puntuaciones de las que fueron aplicadas en el sistema de mando.

Para conseguir cumplir los requisitos, se debe como mínimo cumplir una puntuación de 65, teniendo como máximo sumar 100 puntos en el caso de que se cumplan todos los requisitos.

Nro.	Medida contra el CCF	Puntos
1	Separación/Segregación	
	Separación física entre vias de señal: - Separación de cableado/Tuberías. -Espacios de separación suficientes y distancias de fuga en pistas de circuitos impresos	15
2	Diversidad	
	Uso de diferentes tecnologías,diferentes diseño o principios físicos distintos, por ejemplo: -Primer canal con electrónico programable y segundo canal cableado. -Algún tipo de inicialización. -Presión y temperatura. Medida de distancia y presión. -Digital y analógica. Componentes de diferentes fabricantes.	20
3	Diseño/Aplicación/Experiencia	
3.1	Protección contra sobre corriente, sobrepresión y sobretensión, etc.	15
3.2	Uso de componentes de eficacia probada.	5
4	Evaluación/ Análisis	
	¿se ha tenido en cuenta los resultados de un análisis de modo de fallo y efectos para evitar los CCF durante el diseño?	5
5	Competencia/ Formación	
	¿Tienen formación los diseños y el personal de mantenimiento para entender las causas y consecuencias de los CCF?	5
6	Ambiental	
6.1	Prevención de contaminación y compatibilidad electromagnética (EMC) contra CCF de acuerdo con las normas adecuadas. Sistemas hidrodinámicos: filtración del medio de presión, prevencion de suciedad y contaminación del fluido, drenaje del aire comprimido. Por ej. Cumpliendo las recomendaciones del fabricante de los componentes en lo relativo a la pureza del medio de presión. Sistemas eléctricos: ¿Se ha chequeado el sistema contra inmunidad electromagnética, por ejemplo según lo especificado en las normas relevantes contra los CCF? para sistemas combinados eléctricos e hidrodinámicos, se deben considerar ambos aspectos.	25
6.2	Otras influencias - ¿Se han considerado los requisitos de inmunidad de todas las influencias ambientales relevantes como temperatura, choque, vibración, humedad (por ej. Según lo especificado en las normas relevantes)?	10
	Total	Max. 100

Tabla 1. Tabla de medida contra el CCF

Esta puntuación se suma para determinar el factor de fallo por causa común, como se puede observar en la Tabla 2.

Puntuación general	Factor (β) de fallo por causa común
<35	1 %(0.01)
35...65	0.5 %(0.005)
65...85	0.2 %(0.002)
85...100	0.1 %(0.001)

Tabla 2. Tabla de factor de fallo por causa común

6.2. Cobertura del diagnóstico (DC)

Los sistemas pueden contener pruebas de diagnóstico automáticas, que se utilizan para disminuir la probabilidad de fallos peligros de hardware. El parámetro DC da una idea de cuantos fallos peligrosos detectará el sistema de diagnóstico [32].

Para el valor de la cobertura de diagnóstico se establecen cuatro niveles según se muestra en la Tabla 3:

DESCRIPCIÓN	RANGO
Ninguna	DC $\leq$ 60 %
Baja	60 % $\leq$ DC $\leq$ 90 %
Media	90 % $\leq$ DC $\leq$ 99 %
Alta	99 % $\leq$ DC

Tabla 3. Tabla cobertura de diagnóstico DC

Según se desprende de la tabla, hay tres valores clave en distribución logarítmica: el 60 %, el 90 % y el 99 %. Las siguientes tablas se refieren a los dispositivos de entrada (Tabla 4), dispositivos lógicos (Tabla 5) y dispositivos de salida (Tabla 6).

Medida	Cobertura de Diagnóstico (DC)
Dispositivos de entrada	
Estímulos cíclicos de chequeo en cambios dinámicos en las señales de entrada	90 %
Chequeo de plausibilidad, por ejemplo, usar contactos NA y NC guiados mecánicamente.	99 %
Supervisión cruzada de entradas sin chequeo dinámico	0 % al 99 %, dependiendo de cada cuanto la aplicación realiza un cambio de señal
Supervisión cruzada de señales de entrada con chequeo dinámico si los cortocircuitos no son detectables (para multiples E/S)	90 %
Supervisión cruzada de señales de entrada y resultados intermedios en la lógica (L) y supervisión lógica temporal de software durante el flujo del programa y detección de fallos estáticos y cortocircuitos (para múltiples E/S)	99 %
Supervisión indirecta (por elemplo, supervisión por detectores de presión, supervisión eléctrica de posición de actuadores)	90 % al 99 % dependiendo de la aplicación.
Supervisión directa (por ejemplo supervisión eléctrica de posición de válvulas de control, supervisión de dispositivos electromecánicos por elementos de contactos guiados mecánicamente)	99 %
Detección de defectos por el proceso.	0 % al 99 %, dependiendo de la aplicación; únicamente esta medida por si misma no es suficiente para alcanzar un PLr=e
Supervisión de algunas características del sensor (tiempo de respuesta, rango de señales análogas, por ejemplo por resistencia eléctrica, capacidad, etc.)	60 %

Tabla 4. Tabla de dispositivos de entrada

Medida	Cobertura de Diagnóstico (DC)
Dispositivos Lógico	
Supervisión indirecta (por ej., supervisión por detectores de presión, supervisión eléctrica de posición de actuadores).	90 % al 99 % dependiendo de la aplicación
Supervisión directa (por ej., supervisión eléctrica de posición de válvulas de control, supervisión de dispositivos electromecánicos por elementos con contactos guiados mecánicamente).	99 %
Supervisión simple temporal de los tiempos de ejecución de la lógica (por ej. con temporizadores como watchdog - perro guardián - donde los puntos de disparo están dentro del programa).	60 %.
Supervisión lógica de la parte lógica mediante watchdog (perro guardián), donde el equipo de pruebas realiza chequeos de plausibilidad sobre el comportamiento de la lógica.	90 %
Auto chequeos al arranque para detectar defectos latentes en partes de la lógica (por ej., memorias de datos y programas, puertos de E/S, interfases).	90 % (dependiendo de la técnica de chequeo)
Chequeos de la capacidad de reacción del dispositivo de supervisión (por ej., watchdog o perro guardián) en el canal principal al arranque o cuando se manda la función de seguridad o cuando lo demanda una señal externa a través del sistema de entrada.	90 %
Principio dinámico (todos los componentes de la lógica cambian su estado ON-OFF cuando se demanda la función de seguridad). Por ej., circuitos de enclavamiento implementado con relés.	99 %
Memoria fija: código de control, firma, CRC de doble palabra(8 bits).	90 %
Memoria fija: código de control, firma, CRC de doble palabra(16 bits).	99 %
Memoria variable: chequeo de RAM mediante el uso de datos redundantes, por ej., flags (banderas), marcadores, constantes, temporizadores y comparación cruzada de estos datos.	60 %
Memoria variable: chequeo de legibilidad y capacidad de escritura en células de memoria usadas.	60 %
Memoria variable: supervisión RAM con código Hamming modificado o auto chequeo de RAM (por ej. "Gal pat" o .ᴬbraham").	99 %
Unidad de proceso: auto chequeo por software.	60 % al 90 %
Unidad de proceso: procesamiento codificado.	90 % al 99 %
Deteccción de defectos por el proceso.	0 % al 99 %

Tabla 5. Tabla de dispositivos lógicos

Medida	Cobertura de Diagnóstico (DC)
Dispositivos de salida	
Supervisión de salidas por un canal sin chequeo dinámico.	0 % al 99 %, dependiendo de cada cuanto la aplicación realiza un cambio de señal.
Supervisión cruzada de salidas sin chequeo dinámico.	0 % al 99 %, dependiendo de cada cuanto la aplicación realiza un cambio de señal.
Supervisión cruzada de señales de salida con chequeo dinámico si los cortocircuitos no son detectables (para múltiples E/S).	90 %.
Supervisión cruzada de señales de salida y resultados en la lógica (L) y supervisión lógica y temporal del software durante el flujo del programa y detección de fallos estáticos y cortocircuitos (para multiples E/S).	99 %.
Vía de desconexión redundante sin supervisión del actuador.	0 %.
Vía de desconexión redundante con supervisión de uno de los actuadores realizada por la lógica y por el equipo de chequeo.	90 %.
Vía de desconexión redundante con supervisión de los actuadores realizada por la lógica y por el equipo de chequeo.	99 %.
Supervisión indirecta (por ej., supervisión por detectores de presión, supervisión eléctrica de posición de actuadores).	90 % al 99 % dependiendo de la aplicación.
Detección de defectos por el proceso.	0 % al 99 % dependiendo de la aplicación; únicamente esta medida no es suficiente para alcanzar un PLr=e.
Supervisión directa (por ej., supervisión eléctrica de posición de válvulas de control, supervisión de dispositivos electromecánicos por elementos guiados mecánicamente).	99 %.

Tabla 6. Tabla de dispositivos de salida

Para obtener este parámetro es necesario elegir el nivel de diagnóstico deseado para cada parte del sistema y a partir de estos valores seleccionar el menor como cobertura de diagnóstico (DC).

6.3. Tiempo y probabilidad de fallos peligrosos

El tiempo medio hasta fallo peligroso *(MTTFd)* representa el tiempo sin averías o fallos peligrosos, previsto por un año de operación. Este valor se clasifica en 3 niveles: bajo medio y alto [33]. A su vez, la probabilidad de fallo peligroso por hora *(PFHd)*, se relaciona como el inverso del $MTTFd$, siendo una especia de tasa de fallos peligrosos, como se indica a continuación [33]:

$$PFHd = \frac{1}{MTTFd}$$

6.4. Verificación $PL \geq PLr$ (Requerido)

Se deben satisfacer los niveles de prestaciones requeridos *(PLr)* para cada función de seguridad individual, si no se satisface, es necesario volver a iniciar el proceso y cambiar la función de seguridad que se tenía.

El PL de las diferentes partes del sistema de mando referente a la seguridad, deben ser superiores o iguales al nivel requerido obtenido mediante el árbol de selección [29]. Esto se realiza hallando el PL mediante la gráfica presentada en la figura 10:

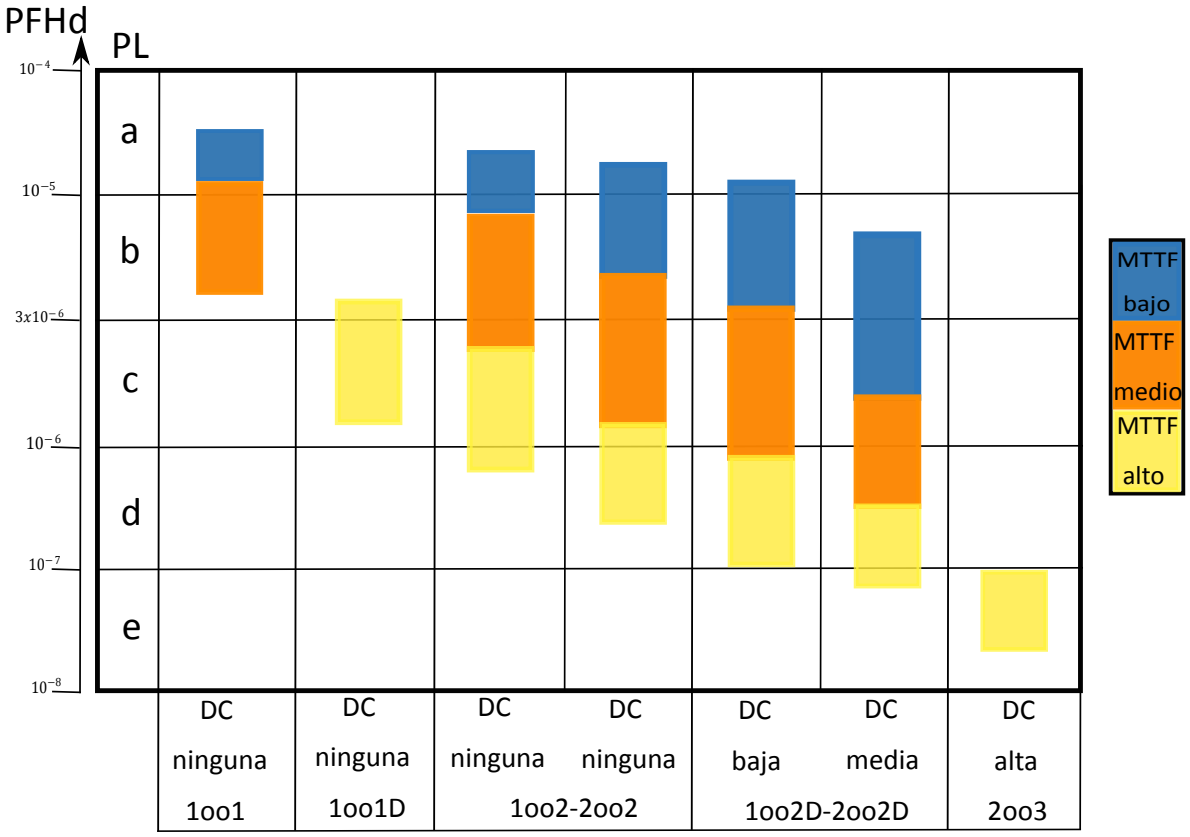


Figura 10. Obtención *PL* total del sistema. Fuente el autor.

En esta figura se relacionan los diferentes parámetros descritos anteriormente, mediante los cuales se puede obtener el valor del *PL* total del sistema o de sus partes. Como se observa, se tienen todas las condiciones posibles de cada uno de los parámetros, es decir el tipo de DC, la categoría a la cual corresponde, el nivel del *MTTF* que se tiene y el valor del *PFHd*. Dependiendo de donde se crucen todos estos parámetros en el gráfico, se obtiene un valor muy aproximado, o casi exacto, del nivel de prestaciones *(PL)*.

7. TIPOS DE ARQUITECTURAS PARA LOS SISTEMAS DE SEGURIDAD

Existen diferentes arquitecturas básicas para sistemas de seguridad:

Arquitectura 1oo1: es una configuración simple con una sola entrada y una única salida sin protección contra modos de fallo [29] [34], como se muestra gráficamente en la figura 11.

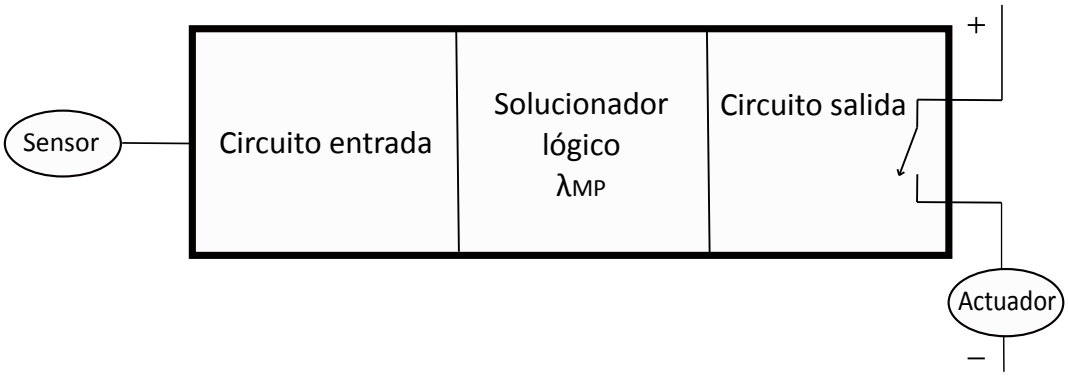


Figura 11. Arquitectura 1oo1. Fuente el autor.

En este tipo de arquitectura, el sistema falla cuando algún elemento de la función de seguridad falla. Un ejemplo sencillo es cuando se tiene un motor eléctrico funcionando gracias al cierre de un contacto, sin embargo, cuando se desea desactivar el motor, el contacto no responde, por lo cual el actuador se mantiene activo.

Arquitectura 1oo1D: es igual que la arquitectura 1oo1 adicionando capacidad de diagnóstico y un segundo canal en serie, que usa la citada señal de diagnóstico, para abrir la salida (la salida solo actúa ante fallo por diagnóstico) [29], ver figura 12.

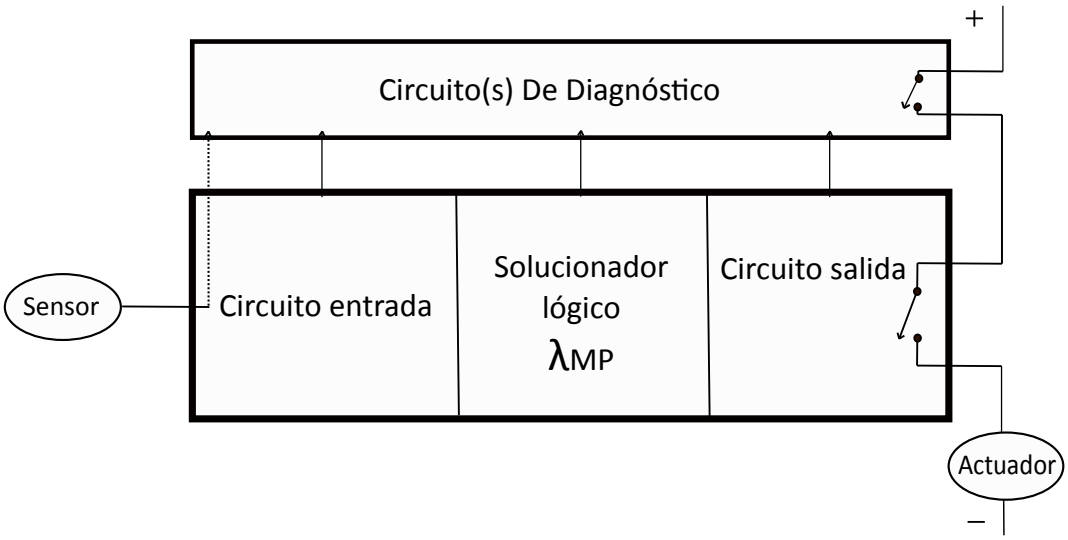


Figura 12. Arquitectura 1oo1D. Fuente el autor.

Arquitectura 1oo2: este tipo de arquitectura se utiliza para minimizar fallos peligrosos. Gracias a la conexión serie de sus salidas, ver figura 13, ambos canales deben fallar de forma peligrosa para ocasionar falla peligrosa. Sin embargo, incrementa probabilidad de fallas en modo seguro [29] [34].

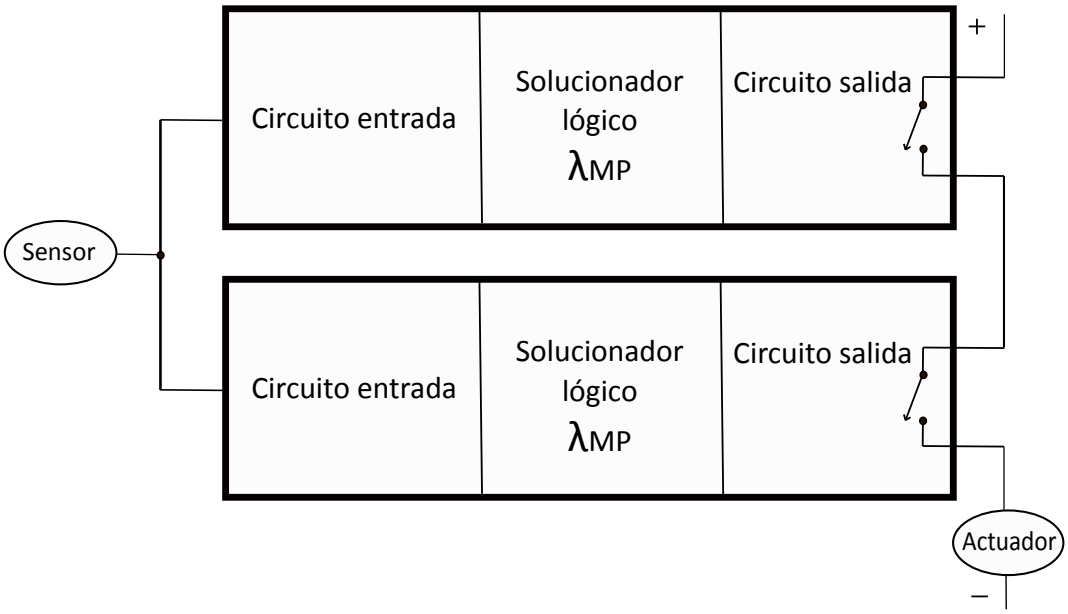


Figura 13. Arquitectura 1oo2. Fuente el autor.

En este tipo de arquitectura, la función de seguridad fallará solo si ambos relés no consiguen abrirse; si uno de los dos puede efectuar la apertura se logra el bloqueo del sistema (des energizar el actuador). Por ejemplo, en un proceso en el cual se maneja un líquido peligroso y es necesario el cierre de actuadores, como válvulas, para evitar algún accidente, es posible utilizar la arquitectura 1oo2, ya que en el momento de fallo aunque una de las dos válvulas no funcione adecuadamente, se tiene otra de respaldo.

Arquitectura 1oo2D: es igual a 1oo2 más diagnóstico. Permite que una falla peligrosa no detectada en una unidad, sea bloqueada por la unidad operativa, como se indica en la figura 14. Funciona bien con todos los contactos de salida cerrados [29].

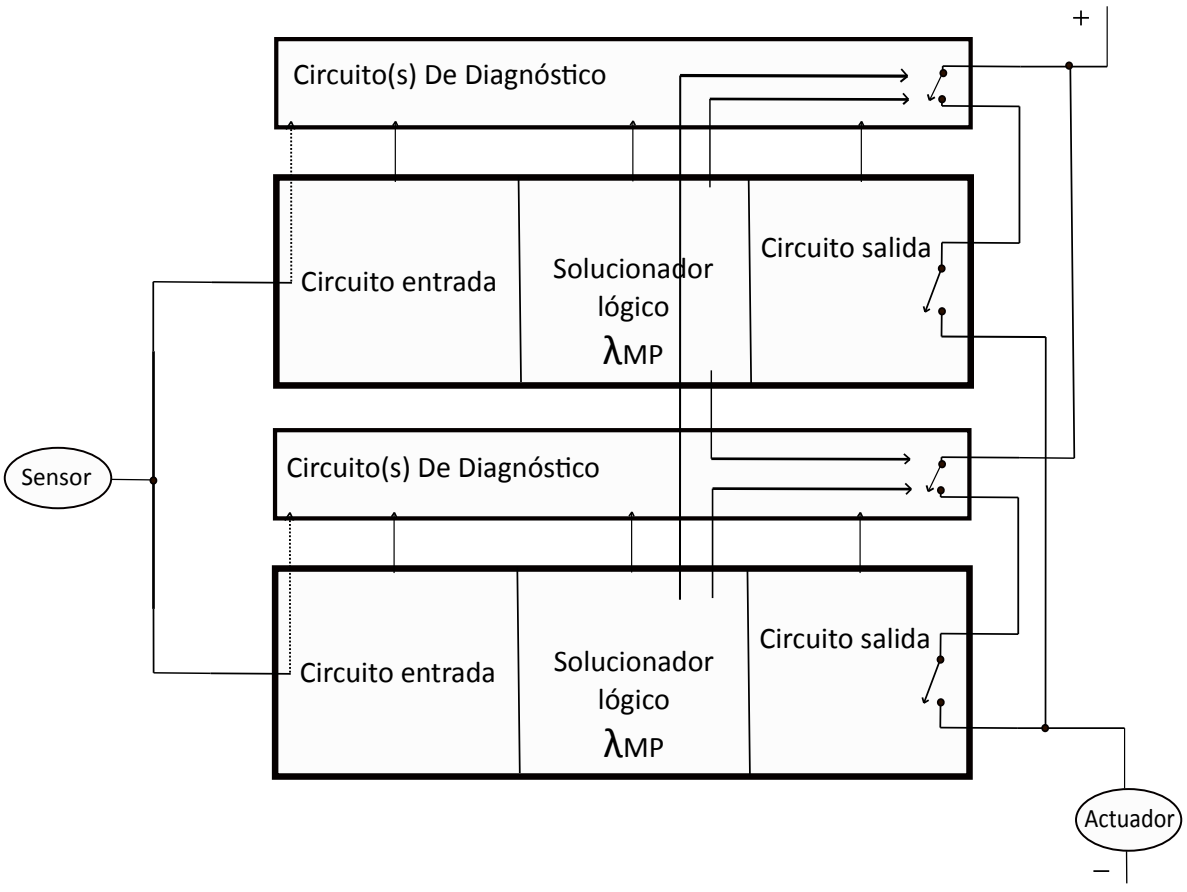


Figura 14. Arquitectura 1oo2D. Fuente el autor.

Arquitectura 1oo3: es un sistema de triple redundancia, que se usa sólo para aplicaciones en las que se exija un funcionamiento seguro durante largos períodos, es decir que los sistemas o las máquinas no pueden ser detenidos para pruebas y mantenimientos durante 5 o más años. Otra aplicación es alcanzar el nivel de integridad de la seguridad SIL 3 [29].

Arquitectura 2oo2: este tipo de arquitectura se utiliza en situaciones donde no se desea fallar con las salidas abiertas (fallos seguros). Sus salidas están cableadas en paralelo y si un controlador falla con su salida abierta, el otro aún es capaz de energizar la carga (actuador). Sin embargo, es susceptible a fallas en las cuales la salida está energizada [29], ver figura 15.

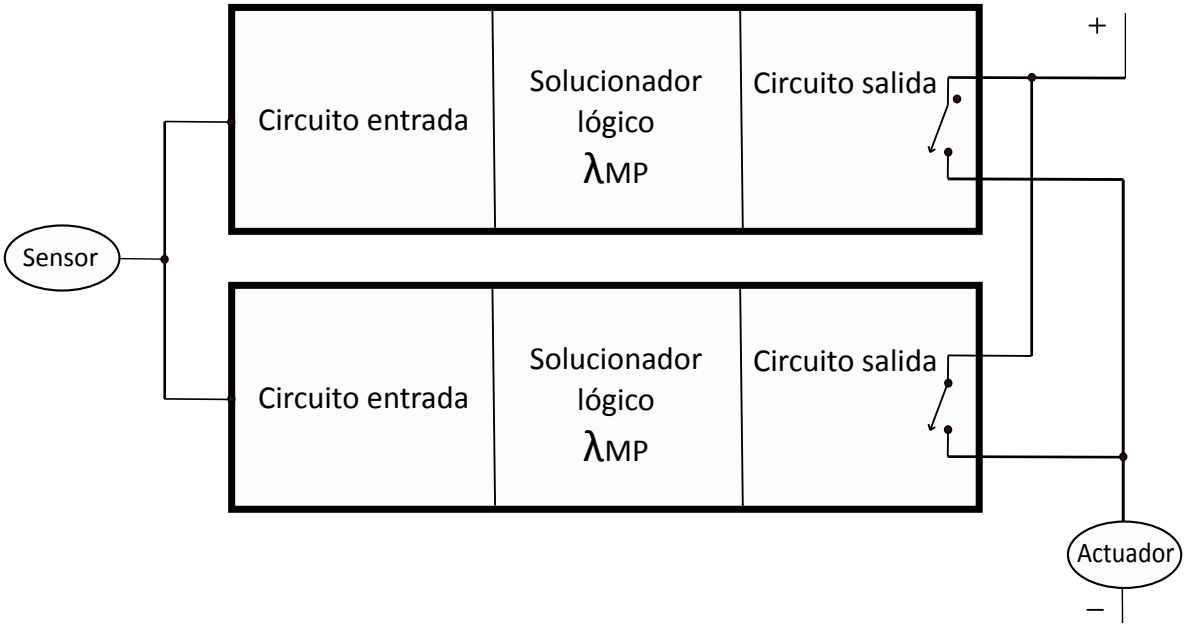


Figura 15. Arquitectura 2oo2. Fuente el autor.

Este tipo de arquitectura se utiliza para energizar diferentes tipos de actuadores en procesos industriales donde es necesario evitar accidentes o retrasos en el inicio de procesos, los cuales generan pérdidas económicas.

Arquitectura 2oo2D: consiste de 2 controladores 1oo1D en arreglo tipo 2oo2, como se observa en la figura 16. Esta configuración permite proteger contra apagados y provee diagnóstico [29].

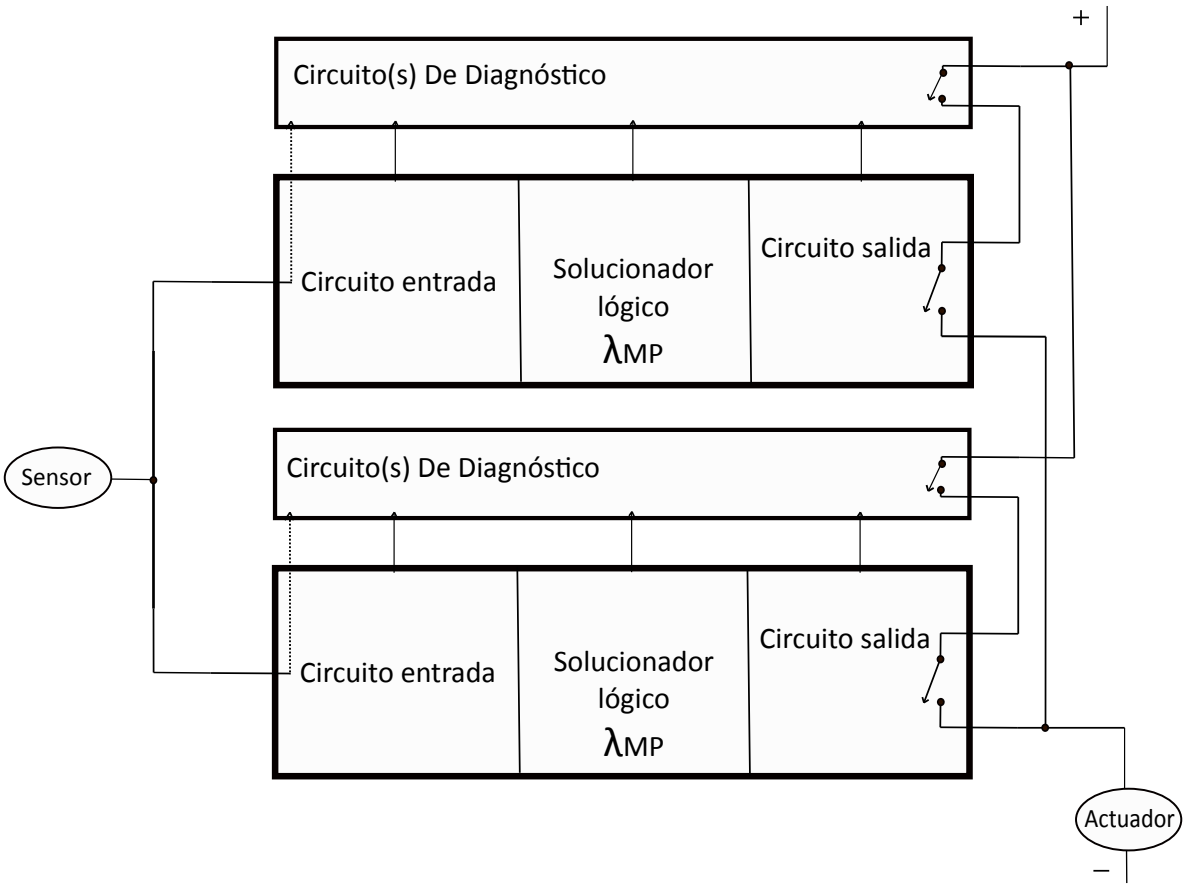


Figura 16. Arquitectura 2oo2D. Fuente el autor.

Arquitectura 2oo3: esta es una configuración tolerante a fallos seguros y a fallos inseguros. Como se observa en la figura 17, es un sistema de votación por ramales de a 2 salidas, desde 2 controladores cada vez. Funciona con mayoría simple, es decir, lo que indican 2 o más entradas, es lo que el sistema adopta. No es mejor que 1oo2 para fallos inseguros, ni que 2oo2 para fallos seguros, sin embargo, 2oo3 es válida para fallos seguros e inseguros [29].

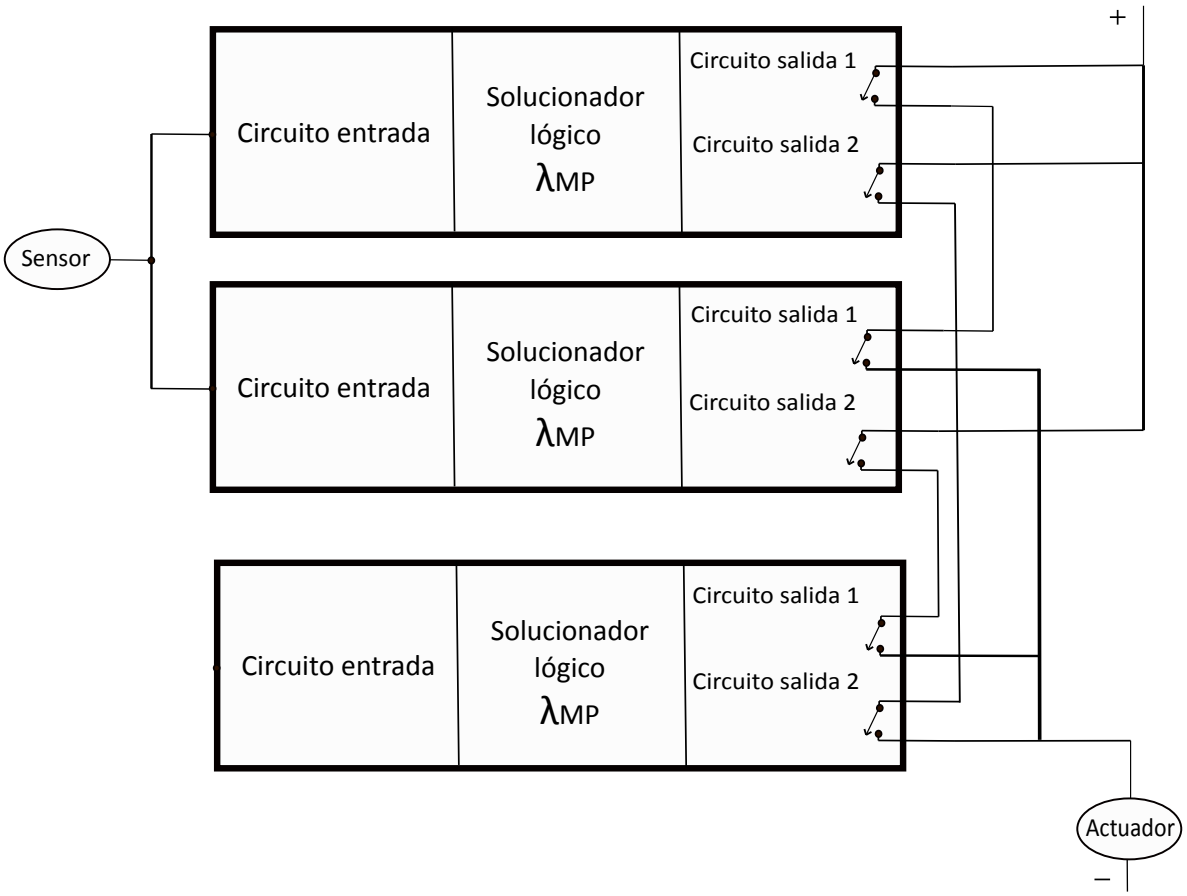


Figura 17. Arquitectura 2oo3. Fuente el autor

8. CADENAS DE MARKOV

En este apartado, se presentan las cadenas de Markov como medio para el modelamiento y descripción de mantenimiento predictivo en espacio de estados.

En este escenario, los sistemas no reparables evalúan la confiabilidad bajo la premisa que a dichos sistemas no se les realiza ningún tipo de intervención hasta su fallo, o hasta su mantenimiento preventivo. Esto ocurre ya sea por la filosofía de mantenimiento que se implementa, o por que el sistema no permite tratar el fallo con el sistema operando, lo cual es común cuando los sistemas no poseen redundancia, o solo permitan intervenciones en frío, es decir, cuando el sistema está en paro.

Los sistemas con algún tipo de redundancia (activa, k de n:G, stand by, etc.) pueden permitir (no siempre) realizar reparación de unidades en falla, sin necesidad de parar la operación del sistema (o, reparación en caliente). Para estos sistemas, los modelos con base en redes de confiabilidad fallan en representar la reparación en caliente. Es acá donde las cadenas de Markov se presentan como un modelo adecuado para representar las actividades de reparación en caliente, en sistemas que poseen algún medio de redundancia.

8.1. Modelo de sistemas reparables con Markov

Un modelo por cadenas de Markov, es un sistema de representación de la operación por espacio de estados; en las cadenas de Markov es posible realizar transiciones de estado a estado mediante las tasas de fallo (λ, representa la transición a un estado de fallo) y las tasas de reparación (μ, representa el retorno de cualquier estado de fallo al precedente) de los distintos elementos del sistema. A medida que se desarrolla el diagrama de Markov se introducen los valores de fallos y reparación en una matriz n x

n (siendo n el número de estados) conocida como matriz de transición, con la cual es posible calcular la probabilidad de permanecer en cada uno de los estados. Por ejemplo, si un sistema cuenta con dos unidades en paralelo, el sistema opera con una unidad funcional y la otra en falla; pero la unidad en falla se puede reparar mientras la otra da soporte. En el caso del ejemplo anterior, el sistema se representa en la figura 18, con los siguientes estados de operación [35]:

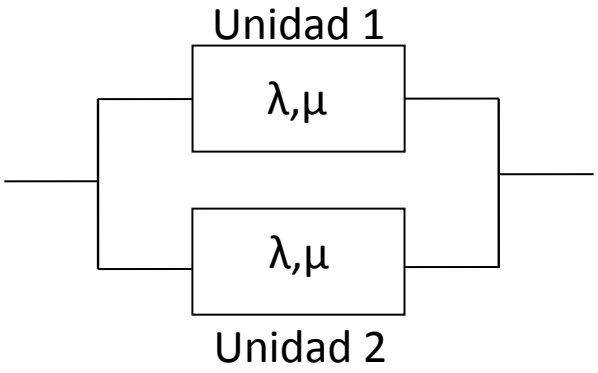


Figura 18. Sistema con dos unidades funcionales. Fuente el autor.

Estado (0): ambas unidades cumplen función requerida (sistema funcional).
Estado (1): una unidad opera y la otra unidad está en falla (sistema funcional).
Estado (2): ambas unidades en falla y el sistema no es funcional.

Con base en este sistema de ejemplo, a continuación se muestra el procedimiento para evaluación del *MTBF*. Este procedimiento luego será extendido a cualquier sistema.

Suposiciones del modelo:

Si el tiempo de evaluación es en intervalos muy pequeños, se puede despreciar la ocurrencia de dos eventos de fallo simultáneos. Desde un punto de vista de probabilidad condicional, esto es:

$$P(t \leq T \leq t + \frac{\Delta t}{T} > t) = \frac{F(t + \Delta t) - F(t)}{1 - F(t)} = 1 - \frac{R(t + \Delta t)}{R(t)}$$

$$P(t \leq T \leq t + \frac{\Delta t}{T} > t) = 1 - \frac{e^{-}\lambda(t + \Delta T)}{e^{-\lambda t}} = 1 - e^{-}\lambda\Delta t \approx \lambda\Delta t$$

Si para una unidad λ = 0,0001fallos/hora y Δ t = 0,1h (6 min), entonces la probabilidad de falla de la unidad es: $Q(\Delta\ t)$ = 1 - $R(\Delta\ t)$ = 1 - exp -λ * $\Delta\ t$ = 0,00000099 lo que aproximadamente es igual a λ * $\Delta\ t$ = 0,0001 * 0,01 = 0,000001. Si con estas dos unidades se arma un sistema en redundancia, entonces la probabilidad de fallo simultanea de las dos unidades es: $Q(\Delta\ t) = Q(\Delta t)$ * $Q(\Delta t) = 9,8 * 10^{-13} \approx = 0$.

De lo anterior, la probabilidad de la falla de una única unidad se puede aproximar a $Q(\Delta t) \approx = \lambda^{*}\Delta t$.

Otra consecuencia de lo anterior es que la probabilidad de falla simultánea de dos unidades (o más) en redundancia se puede aproximar a $Q(\Delta t) \approx = 0$. Lo anterior también se puede expresar diciendo que los eventos de fallo son mutuamente excluyentes (si ocurre un fallo, no puede ocurrir otro simultáneamente).

El modelo de Markov hará las anteriores aproximaciones aún más efectivas a medida que $\Delta t \longrightarrow 0$.

Todas las anteriores suposiciones y aproximaciones se resumen en la denominada Propiedad Markoviana: La probabilidad de transición de un estado a otro únicamente depende del estado en sí, es decir, la probabilidad de falla no depende de la historia pasada del sistema.

Dada que la evaluación se hace a intervalos pequeños de tiempo, el modelo supone tasa de fallos constante λ y tasa de reparación constante μ.

Lo que se desea evaluar es la probabilidad de permanecer en cada uno de los estados, notado como *Pi(t)*, donde i es el subíndice que hace referencia a un estado en particular y t es el instante de tiempo. Se asume que el instante inicial para evaluación del tiempo

es (0), por tanto, al inicio el sistema debe estar en el Estado (0), o debe ser funcional con todas las unidades operando (2 en este caso), y en el infinito debe estar en el último estado, o Estado (2) en este caso, ya que debe estar no funcional con todas las unidades en falla [35]. Lo anterior se conoce como las condiciones de frontera del modelo, y se escriben como:

$$P_0(0) = 1; P_1(0) = P_2(0) = 0$$

$$P_2(\infty) = 1; P_0(\infty) = P_1(\infty) = 0$$

Además, por ser probabilidades se cumple que:

$$P_0(t) + P_1(t) + P_2(t) = 1$$

De todo lo anterior, la probabilidad de falla de una sola unidad es $Q(\Delta t) \approx= \lambda\Delta t$, y la confiabilidad o probabilidad de no falla, de una sola unidad es: $R(\Delta t) = 1 - Q(\Delta t) \approx = 1\text{-}\lambda\Delta t$.

La probabilidad de no falla de dos unidades en paralelo es: $R(\Delta t) = (1 - \lambda\Delta t)(1 - \lambda\Delta t)$, que resolviendo lleva a $R(\Delta t) = 1\text{-}2\lambda\Delta t + [\lambda\Delta t]2 = 1\text{-}2\lambda\Delta t$.

Finalmente, la probabilidad de falla de dos unidades en paralelo es: $Q(\Delta t) = 1 - R(\Delta t) = 1 - (1 - 2\lambda\ \Delta t) = 2\lambda\ \Delta t$, y la probabilidad de reparación de una unidad es $\mu\ \Delta t$. Con los anteriores datos, producto de las suposiciones del modelo de Markov, se puede proceder a evaluar la probabilidad de encontrar el sistema en cada uno de sus posibles estados, así:

Probabilidad de estar en el Estado (0):

La probabilidad que el sistema se encuentre en el estado (0) en el instante de tiempo

$t + \lambda t$ depende de si: el sistema estaba en t en el estado (0) y no ocurrieron fallas en ninguna de las dos unidades durante el intervalo λt, o el sistema estaba en t en el estado (1) y durante el intervalo λt no falló la unidad funcional y se reparó la unidad en fallo. Estas condiciones se pueden expresar como:

$$P_0(t + \Delta t) = P_0(t) * (1 - 2\lambda\Delta t) + P_1(t) * (1 - \lambda\Delta t)(\mu\Delta t)$$

Organizando, se tiene:

$$\frac{P_0(t + \Delta t) - P_0(t)}{\Delta t} = -2\lambda P_0(t) + \mu P_1(t)$$

Y al aplicar el límite cuando $\Delta t \longrightarrow 0$, se obtiene:

$$P_0'(t) = -2\lambda P_0(t) + \mu P_1(t)$$

Probabilidad de estar en el Estado (1):

La probabilidad que el sistema se encuentre en el estado (1) en el instante de tiempo $t + \Delta t$ depende de si: el sistema estaba en t en el estado (0) y falla una de las dos unidades durante el intervalo Δt, o el sistema estaba en t en el estado (1) y durante el intervalo Δt no fallo la unidad funcional y no se repa la unidad en fallo. Estas condiciones se pueden expresar como:

$$P_1(t + \Delta t) = P_0(t) * (2\lambda\Delta t) + P_1(t) * (1 - \lambda\Delta t)(1 - \mu\Delta t)$$

Organizando, se logra:

$$\frac{(P_1(t+\Delta t) - P_1(t))}{\Delta t} = 2\lambda P_0(t) - (\lambda + \mu)P_1(t)$$

Y al aplicar el límite cuando $\Delta t \longrightarrow 0$, se obtiene:

$$P_1'(t) = 2\lambda P_0(t) - (\lambda + \mu)P_1(t)$$

Probabilidad de estar en el Estado (2):

La probabilidad que el sistema se encuentre en el estado (2) en el instante de tiempo $t + \Delta t$ depende de si: el sistema estaba en t en el estado (1) y durante el intervalo Δt falló la unidad funcional y no se reparó la unidad en fallo, o el sistema ya estaba en t en el estado (2). Las condiciones previas se pueden expresar como:

$$P_2(t+\Delta t) = P_1(t) * (\lambda \Delta t)(1 - \mu \Delta t) + P_2(t)$$

Organizando, se obtiene:

$$\frac{(P_2(t+\Delta t) - P_2(t))}{\Delta t} = \lambda P_1(t)$$

Y al aplicar el límite cuando $\Delta t \longrightarrow 0$, se llega a:

$$P_2'(t) = \lambda P_1(t)$$

Matricialmente, las tres ecuaciones previas quedan de la siguiente forma, donde [M] es la denominada matriz de Markov:

$$\begin{bmatrix} P_0'(t) \\ P_1'(t) \\ P_2'(t) \end{bmatrix} = \begin{bmatrix} -2\lambda & \mu & 0 \\ 2\lambda & -(\lambda+\mu) & 0 \\ 0 & \lambda & 0 \end{bmatrix} \begin{bmatrix} P_0(t) \\ P_1(t) \\ P_2(t) \end{bmatrix} \quad \left[P'\right] = \left[M\right]\left[P\right]$$

La matriz $[M]$ se puede representar en un diagrama de transición de estados, como se indica en la figura 19, así:

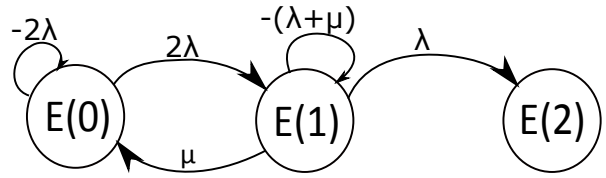


Figura 19. Representación por estados. Fuente el autor.

La matriz, en general, indica la suma de probabilidades de falla, o de reparación, entre estados. La probabilidad de permanencia en cada estado es la suma de los valores de salida del mismo estado.

Un sistema reparable es confiable cuando se encuentra en cualquier estado donde el sistema sea funcional. El sistema de ejemplo con 2 unidades en paralelo es confiable en los estados 0 y 1; en el estado 2 el sistema es inconfiable. Para este modelo, el estado E(2) se comporta como un estado absorbente, representando la llegada a una estado de fallo. La matriz de Markov previa representa la situación descrita [36].

Entonces, el modelo para confiabilidad tiene ceros en columna del estado final y el modelo de estados no posee salidas ni permanencia en el estado final.

$$\left[M\right] = \begin{bmatrix} -2\lambda & \mu & 0 \\ 2\lambda & -(\lambda+\mu) & 0 \\ 0 & \lambda & 0 \end{bmatrix}$$

El modelo confiabilidad, o de mantenibilidad, permite determinar el tiempo promedio entre fallos ($MTBF$), o $\varnothing_S$ del sistema al que se le realiza reparación en caliente, al solucionar el sistema $[P] = [M][P]$. Ya que, para el ejemplo, el sistema no es confiable (no es funcional) en el estado $P_2(t)$, se tiene:

$$\varnothing_S = \int_0^\infty R(t)dt = \int_0^\infty [P_0 + P_1]dt$$

$$\varnothing_S = \int_0^\infty P_0(t)dt + \int_0^\infty P_1(t)dt = T_0 + T_1$$

Para solucionar, y sabiendo que $[M]$ es una constante, se debe resolver:

$$\int_0^\infty [P']dt = [M] \int_0^\infty [P]dt$$

Integrando:

$$\begin{bmatrix} \int_0^\infty P_0'(t)dt \\ \int_0^\infty P_1'(t)dt \\ \int_0^\infty P_2'(t)dt \end{bmatrix} = \begin{bmatrix} -2\lambda & \mu & 0 \\ 2\lambda & -(\lambda+\mu) & 0 \\ 0 & \lambda & 0 \end{bmatrix} \begin{bmatrix} \int_0^\infty P_0(t)dt \\ \int_0^\infty P_1(t)dt \\ \int_0^\infty P_2(t)dt \end{bmatrix}$$

$$\begin{bmatrix} P_0(\infty) - P_0(0) \\ P_1(\infty) - P_1(0) \\ P_2(\infty) - P_2(0) \end{bmatrix} = \begin{bmatrix} -1 \\ 0 \\ 1 \end{bmatrix} \begin{bmatrix} -2\lambda & \mu & 0 \\ 2\lambda & -(\lambda+\mu) & 0 \\ 0 & \lambda & 0 \end{bmatrix} \begin{bmatrix} T_0 \\ T_1 \\ T_2 \end{bmatrix}$$

Al solucionar se tiene que:

$$T_0 = \frac{\lambda + \mu}{2\lambda^2}$$

y

$$T_1 = \frac{1}{\lambda}$$

de donde

$$\varnothing_S = \frac{3\lambda + \mu}{2\lambda^2}$$

Si no hay reparación ($\mu = 0$) se obtiene que $\varnothing_S = 3/2\ \lambda$, que es el mismo *MTBF* para 2 unidades en paralelo y sin reparación. Si la tasa de reparación es cercana a cero, el tiempo de reparación es alto, y el *MTBF* se acerca al de un sistema sin reparación. Si la tasa de reparación es alta, el tiempo de reparación es bajo y el *MTBF* crece.

En la figura 20 se muestra el *MTBF* en un sistema sin reparación (línea negra) contra un sistema con reparación (línea azul), cuando $\lambda = 0{,}001$ y con μ variando desde 0 hasta 0,001. Si $\mu = 0$, el *MTBF* con reparación es igual al *MTBF* sin reparación. A medida que μ crece, el tiempo de reparación se reduce y el *MTBF* se incrementa [35].

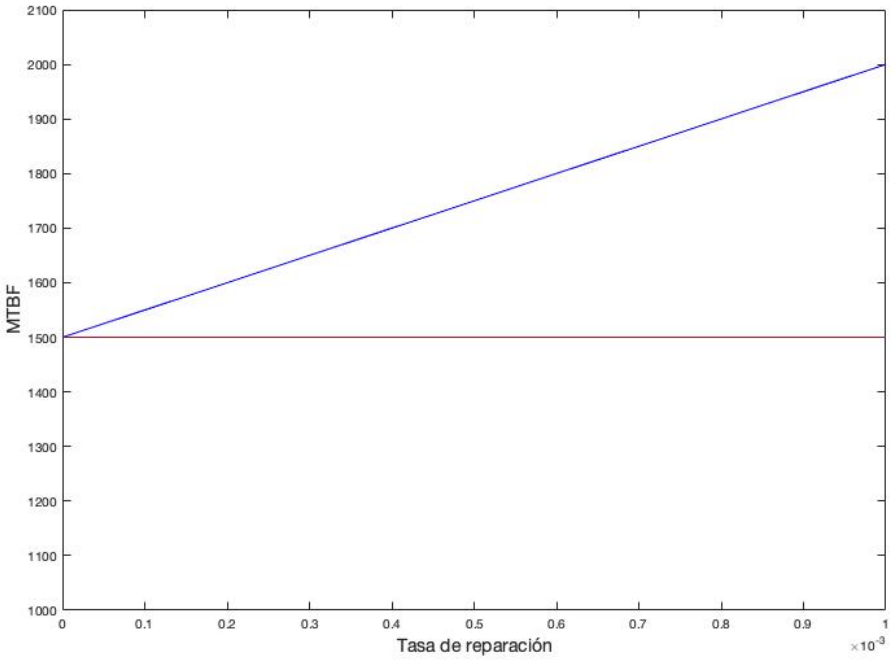


Figura 20. *MTBF* vs Reparación. Fuente el autor.

La *disponibilidad* es la razón producto de dividir el tiempo que el sistema es funcional entre el tiempo que es funcional más el que no lo es. Para evaluar la *disponibilidad* se requiere introducir reparación en el estado final, para evaluar la permanencia en cada estado en operación estable del sistema, como se observa en la figura 21.

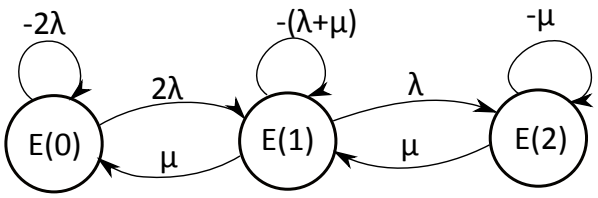


Figura 21. Máquina de estados con reparación en estado final (*disponibilidad*). Fuente el autor.

Ahora, así como el diagrama de estados refleja la reparación en el estado final, la matriz de Markov también lo debe hacer [35], quedando:

$$[M] = \begin{bmatrix} -2\lambda & \mu & 0 \\ 2\lambda & -(\lambda+\mu) & \mu \\ 0 & \lambda & -\mu \end{bmatrix}$$

En el modelo de *disponibilidad* se busca el estado estable en el cual no hay cambios en los valores de probabilidad, $[P'] = [M][P] = 0$. Para solucionar se debe tener cuidado con el hecho que en el sistema, las ecuaciones no son independientes, por lo que se debe agregar la ecuación $P_0(t) + P_1(t) + P_2(t) = 1$. Entonces, la *disponibilidad* es:

$$disponibilidad = P_0(t) + P_1(t) = 1 - P_2(t)$$

Al solucionar se tiene que:

$$disponibilidad = 1 - \frac{2\lambda^2}{2\lambda^2 + \mu^2 + 2\lambda\mu}$$

Si no hay reparación en el estado final, se obtiene que *disponibilidad* = 0, o en el estado estable el sistema estará en falla. Si la tasa de reparación es cercana a cero, el tiempo de reparación es alto y, nuevamente, *disponibilidad* $\approx = 0$. Si la tasa de reparación es alta, ahora el tiempo de reparación es bajo y la *disponibilidad* $\approx = 1$.

En la figura 22, se muestra la *disponibilidad* en un sistema sin reparación (línea negra) contra un sistema con reparación (línea azul), cuando $\lambda = 0{,}001$ y con μ variando desde 0 hasta 0,001. Si $\mu = 0$, la *disponibilidad* con reparación es cero, igual pasa si no hay reparación, ya que *disponibilidad* $= MTBF/(MTBF + MTTR) = \mu/(\lambda + \mu)$. La *disponibilidad* con reparación es mayor a la sin reparación [35].

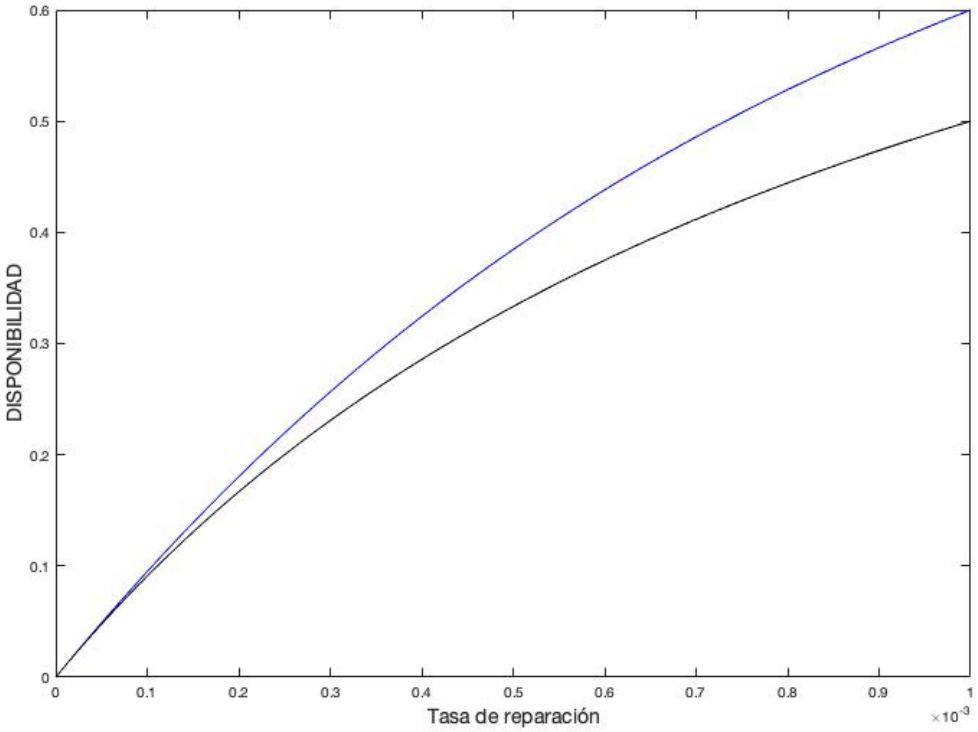
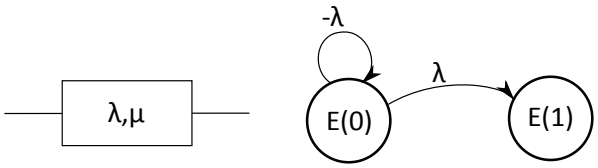


Figura 22. Tendencia de la *disponibilidad* con y sin mantenimiento. Fuente el autor.

En la figura 23 se muestra el modelo de mantenibilidad para una sola unidad y su matriz $[M]$.



$$[M] = \begin{bmatrix} -\lambda & 0 \\ \lambda & 0 \end{bmatrix}; \begin{bmatrix} -1 \\ 1 \end{bmatrix} = \begin{bmatrix} -\lambda & 0 \\ \lambda & 0 \end{bmatrix} \begin{bmatrix} T0 \\ T1 \end{bmatrix}$$

Figura 23. Diagrama de transición de estados de Mantenibilidad. Fuente el autor.

Al solucionar este sistema, se obtiene que: $\varnothing_S = T_0 = MTBF = 1/\lambda$. Y se comprueba que los modelos no reparables son un caso especial del modelo de Markov.

8.2. Modelos de mantenimiento: predictivo vs preventivo

Mantenimiento preventivo: es el cuidado y servicio prestado por el personal involucrado en mantenimiento con el objeto de mantener los equipos/activos en estados satisfactorios de operación usando inspecciones sistemáticas, detección y corrección de fallas incipientes o en general con antelación a su ocurrencia o antes que estas se desarrollen en fallas mayores. [35]. El modelo tradicional para evaluar mantenimiento preventivo, se basa en los diagramas de redes de confiabilidad y la realización de intervalos de mantenimiento a periodos constantes de aplicación. En este modelo, los elementos que fallan entre inspecciones, o intervalos de mantenimiento, solo son reparados al final de cada intervalo, teniendo la operación degradada del sistema hasta una nueva inspección. Esos fallos pueden afectar, o variar, la aplicación del sistema integrado de seguridad que se diseñe.

Mantenimiento predictivo: Se basa en la premisa de que un monitoreo regular de las condiciones actuales de las maquinarias, seguimiento a la eficiencia de operación y otros indicadores de las condiciones de operación en conjuntos de máquinas y sistemas

de procesos, entregaran los datos requeridos para asegurar el máximo de intervalo entre reparaciones y minimizar el número de costos de paros no programados en los conjuntos de maquinarias [35]. El mantenimiento predictivo en lugar de confiar en estadística industriales o ciclos promedios de vida de elementos, emplea el monitoreo directo de las condiciones y eficiencia de un sistema para determinar el tiempo medio para fallo actual de cada sistema en planta. Ya que este tipo de enfoque realiza revisión continua y reperación en caliente de los elementos en falla que lo permiten, se muestra como ideal para aplicación en los sistemas de seguridad, dada la naturaleza de los mismos.

Comparación de modelos: A continuación, se realiza una comparación de resultados del tiempo medio entre fallos ($MTBF$) cuando se aplica mantenimiento preventivo y predictivo. La forma de evaluar el $MTBF$, según el tipo de mantenimiento es [35]:

$MTBF$ sin mantenimiento:

$$MTBF = \frac{1}{\lambda total} \sum_{i=1}^{n} \frac{1}{i}$$

$MTBF$ con mantenimiento preventivo:

$$MTBF = \frac{\int_0^y R(T)\, dT}{1 - R(y)}$$

Donde, $\lambda total$ es la tasa de fallos del sistema y el periodo de mantenimiento preventivo se denota por y.

Si el sistema a evaluar posee un $\lambda total$ de $66 * 10^{-6}$ y se desea como objetivo lograr un sistema $2\sigma = 0,9544$ de confiabilidad, se necesitan 4 unidades en redundancia activa (todos los elementos redundantes están activos de forma simultánea). Al realizar el análisis se calculan 4 escenarios: sin mantenimiento preventivo y con mantenimiento preventivo cada 2, 3 y 6 meses. La tabla 7 enseña los valores de $MTBF$ logrados para estos escenarios.

Sin	Mantenimiento preventivo		
Mantenimiento	2 meses	3 meses	6 meses
31565.7	20560000	6676300	1101700

Tabla 7. Tabla de comparación *MTBF*

Por otro lado, al realizar un análisis con mantenimiento predictivo, se calculan 4 escenarios cada uno con un μ de diferente valor (0,00002; 0,00006; 0,00008; 0,0002). Como el sistema consta de 4 unidades en redundancia, se realiza un diagrama de Markov con 5 estados diferentes, como se indica en la figura 24.

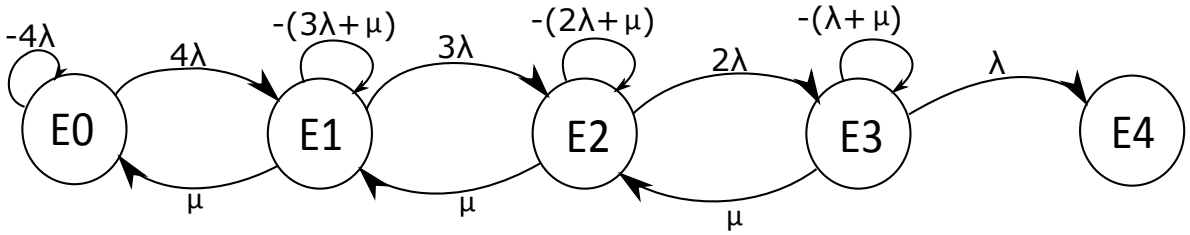


Figura 24. Ejemplo Mantenimiento predictivo. Fuente el autor.

Etapa 0=Todos los elementos funcionan.

Etapa 1=Un elemento presenta falla.

Etapa 2=Dos elementos presentan fallas.

Etapa 3=Tres elementos presentan fallas.

Etapa 4=Todos los elementos en falla.

Este modelo de Markov de 5 estados, se representa entonces por el siguiente sistema matricial:

$$\begin{bmatrix} -1 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} -4\lambda & u & 0 & 0 & 0 \\ 4\lambda & -(3\lambda+u) & u & 0 & 0 \\ 0 & 3\lambda & -(2\lambda+u) & u & 0 \\ 0 & 0 & 2\lambda & -(\lambda+u) & 0 \\ 0 & 0 & 0 & \lambda & 0 \end{bmatrix} \begin{bmatrix} T0 \\ T1 \\ T2 \\ T3 \\ T4 \end{bmatrix}$$

Al resolver la matriz de transición, se obtienen las probabilidades de permanecer en cada estado, así:

$$T0 = \frac{6\lambda^2 + u^3 + \lambda u^2 + 2\lambda^2 u}{24\lambda^4}$$

$$T1 = \frac{2\lambda^2 + u^2 + \lambda u}{6\lambda^2}$$

$$T2 = \frac{\lambda + u}{2\lambda^2}$$

$$T3 = \frac{1}{\lambda}$$

El $MTBF$ se puede definir de la siguiente manera:

$$\phi s = MTBF = T0 + T1 + T2 + T3$$

Obteniendo para este sistema:

$$MTBF = \frac{8\lambda^4 + u^3 + 36\lambda^3 + 4\lambda^3 u + 14\lambda^2 u + 4\lambda^2 u^2 + \lambda u^2 + 6\lambda^2}{24\lambda^4}$$

La ecuación anterior describe el $MTBF$ del sistema propuesto con mantenimiento predictivo. Para observar su comportamiento, se evalúa el $\lambda = 66 * 10^{-6}$ constante y se varía la tasa de reparación (μ) entre 0 y $1 * 10^{-3}$, como se puede observar en la figura 25 en trazo verde; igualmente en esta figura se muestra en trazos de tonos azules el $MTBF$ para mantenimiento preventivo a 2, 3 y 6 meses.

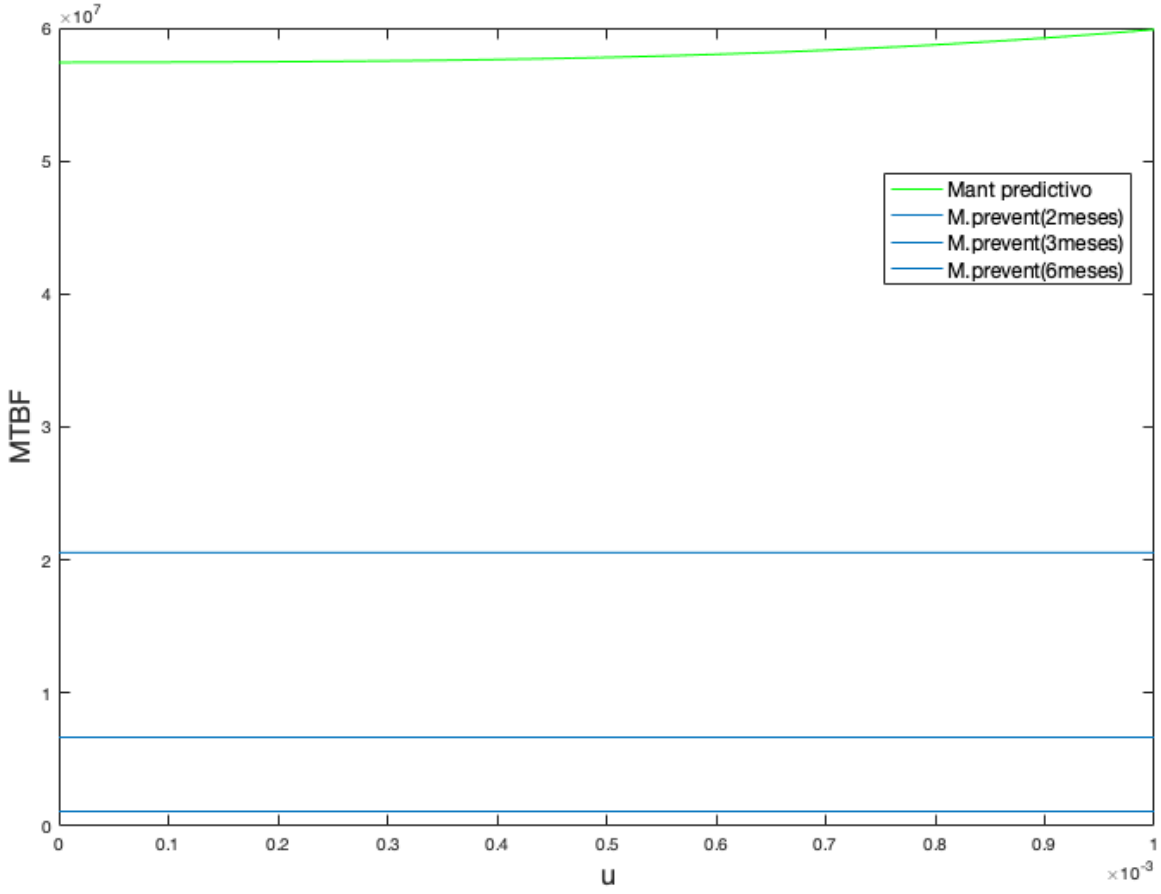


Figura 25. Gráfica $MTBF$ 2. Comparativo de mantenimiento preventivo y predictivo

En la gráfica anterior (figura 25) es posible observar que cuando el sistema cuenta con un mantenimiento predictivo el tiempo medio entre fallos ($MTBF$) es mucho mayor y varía exponencialmente a medida que se incrementa la tasa de reparación (μ), algo que no ocurre con el mantenimiento preventivo, ya que este presenta un valor constante en cualquier valor de μ.

De lo anterior, se evidencia la necesidad de modelar mediante mantenimiento predictivo, y especialmente cuando los componentes del sistema demandan reparación en caliente. Si se modela un sistema mediante mantenimiento preventivo, se asume que las reparaciones solo ocurren al final de cada periodo de revisión, y en el caso de sistemas de seguridad, habría pérdida de la función de seguridad.

9. RESULTADOS, DISCUSIÓN Y CONCLUSIONES

En este capítulo, se expone inicialmente el procedimiento sugerido por norma para la evaluación y verificación del *PLr* requerido por una función de seguridad. En este procedimiento de norma, la obtención del *PFHd* se deja como procedimiento a consideración del diseñador, pero en este trabajo se propone emplear modelos de cadenas de Markov para representar las arquitecturas de los sistemas y evaluar con su ayuda el *PFHd*.

9.1. Procedimiento sugerido por norma

Las normas IEC 61508 e IEC 61511, proponen unos pasos a seguir, con el fin de realizar el proceso de diseño y verificación del *PLr*. Los pasos a seguir son:

1. Identificar y definir requisitos de las funciones de seguridad (SF).

2. Determinar el *PL* requerido (*PLr*).

3. Diseñar e identificar las partes del sistema de mando relativas a seguridad.

4. Determinar el *PL* de las partes del sistema de mando relativas a seguridad.

- Aspectos cuantificables (arquitectura, *MTTFd*, DC, CCF).

- Aspectos no cuantificables.

5. Verificar que $PL \geq PLr$. De lo contrario, rediseñar.

6. Validación.

Es en el paso 4 de la anterior metodología, donde se propone emplear el análisis por cadenas de Markov para calcular el *MTTFd*, con el cual es posible encontrar la probabilidad de fallos por hora (*PFHd*).

9.2. Metodología para realizar un diagrama de Markov para las arquitecturas

De acuerdo con lo expuesto en las capítulos previos, se puede presentar un pseudocódigo para definir los estados involucrados en una cadena de markov que modela una arquitectura específica, según se presenta a continuación:

Pseudocódigo 1: Definir estados

```
Proceso Definir estados de Markov para arquitectura
Inicializar
  j = cantidad de canales del sistema
  k = cantidad elementos por canal

E(0); estado inicial todos los elementos operan

FOR m -> 1 to k
    Crear E(k); fallo del elemento m, del canal 1
END FOR

IF n>1
    FOR n -> 2 to j
        FOR m -> 1 to k
            Crear E(j,k); fallo del elemento k, del canal j
        END FOR
    END FOR
END IF
```

```
IF hay diagnostico
    Crear E(D); estado para fallos de causa comun
END IF
```

Ejemplo, Arquitectura 1oo1: La figura 26 muestra el diagrama de Markov para la arquitectura 1oo1. En este ejemplo, la arquietctura es de un solo canal y sin diagnóstico, por lo que se tiene un estado inicial de operación correcta y tres estados adicionales que representan la falla de cada uno de los elementos del canal (sensor, solucionador lógico y actuador). Desde el estado inicial se va a cada estado con la tasa de fallo respectiva del elemento y se regresa con el inverso del tiempo de reparación, que en este caso es la suma del tiempo de pruebas de diagnóstico (T2) y del tiempo medio de reparación. Ya que este sistema no posee canal de comprobación (diagnóstico), los fallos que se presentan son fallos no detectados y por consiguiente se hace necesario la aplicación de las pruebas de diagnóstico, lo cual queda reflejado en el tiempo T2.

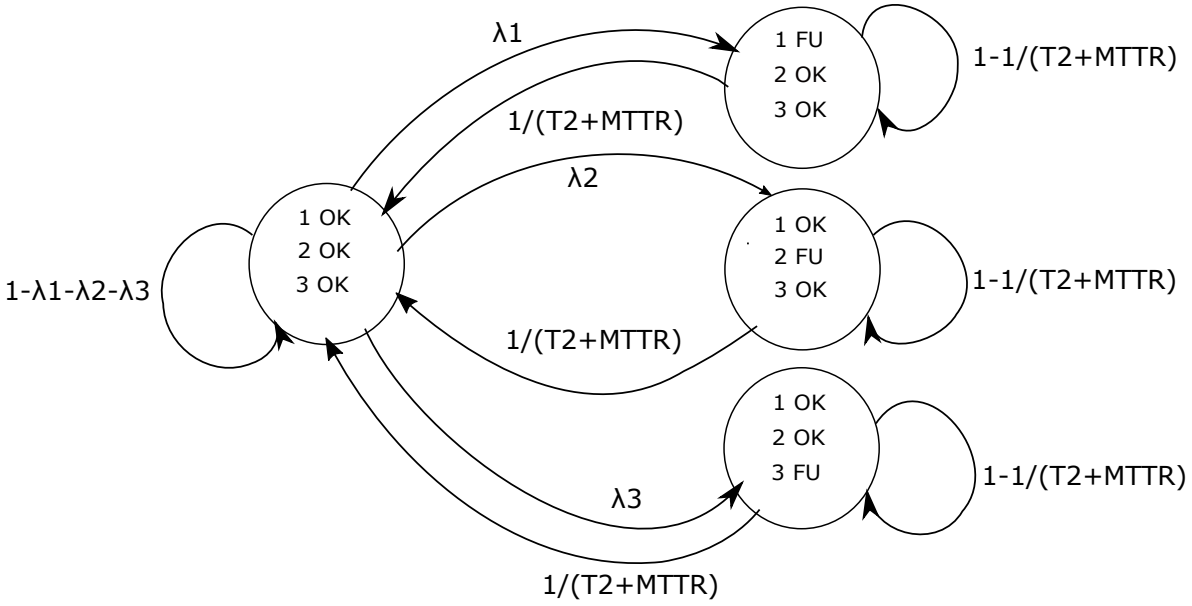


Figura 26. Diagrama Markov 1oo1. Fuente el autor.

Ejemplo, Arquitectura 1oo1D: El diagrama de Markov para la arquitectura 1oo1D se puede observar en la figura 27. Como esta arquitetcura posee diagnóstico, el diagrama está compuesta por cinco estados, así: uno inicial, tres para representar los fallos de los componentes del canal y uno estado adicional que representa los fallos de causa común que efectan al diagnóstico. A cada estado que representa la falla de un elemento, se llega desde el estado inicial con su tasa de fallos respectiva. En esta cadena de Markov, al existir un diagnóstico, los fallos que se presentan son fallos detectados y no se hace necesario aplicar pruebas de comprobación para el canal principal, y únicamente se utiliza T2 para los fallos derivados por causa común (FCC), ya que no es posible detectarlos. Al estado de fallos de causa común se llega mediante la transición β, la cual representa la probabilidad que existe de tener un fallo por causa común en todo el sistema, que por lo general es muy pequeña en comparación con las probabilidades de fallo en un elemento específico. Además, la probabilidad de que no se presente un fallo por causa común (1- β), debe multiplicar las tasas de fallo de cada elemento.

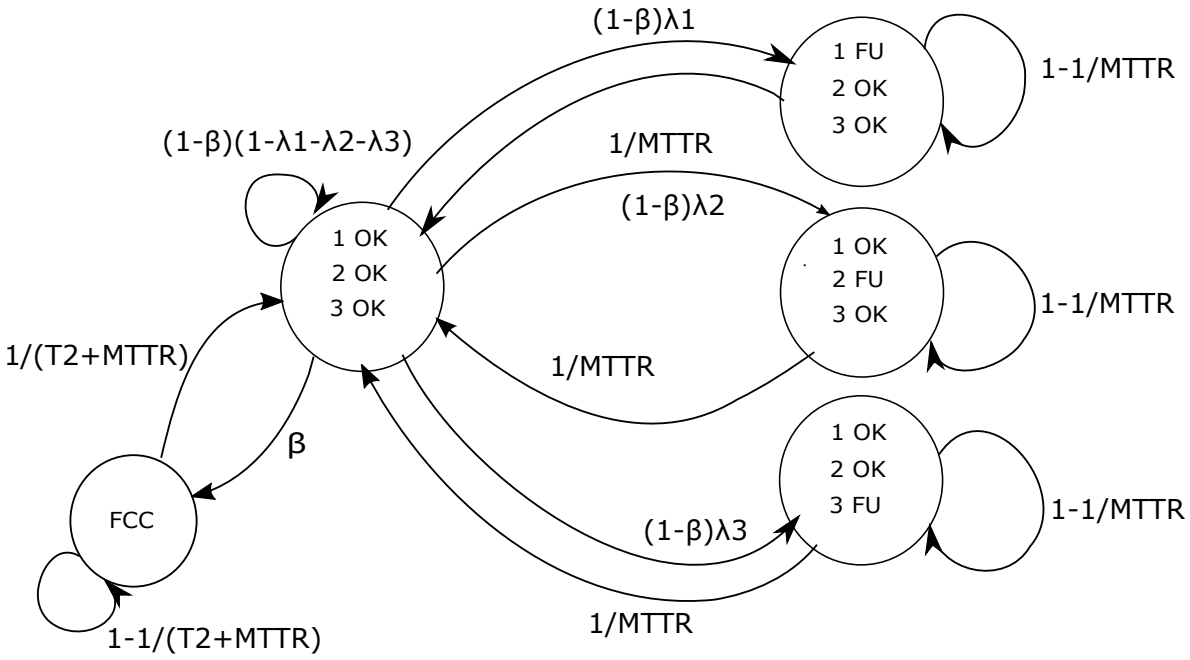


Figura 27. Diagrama Markov 1oo1D. Fuente el autor.

9.3. Metodología para encontrar el *PFHd*

Para encontrar el *PFHd* de una arquitectura, se emplea el modelo derivado de aplicar el Pseudocódigo 1, y definido por los estados de operación, con valores de transición según el siguiente pseudocódigo:

Pseudocódigo 2: Definir transiciones y encontrar *PFHd*

```
Proceso Definir transiciones modelo de Markov para arquitectura
Inicializar
  j = cantidad de canales del sistema
  k = cantidad elementos por canal
Entradas
  Conjunto de estados del sistema

IF NO hay diagnostico
    FOR m -> 1 to k
        Transicion(E(0),E(k))= lambda k;
        Transicion(E(k),E(0))= 1/(T2+MTTR);
    END FOR
    IF n>1
        FOR n -> 2 to j
            FOR m -> 1 to k
                Transicion(E(n-1),E(n,m))= lambda n,m;
            END FOR
        END FOR
        Transicion(E(j,k),E(0))= 1/(T2+MTTR);
    END IF
```

```
    Transicion(E(z),E(z))=1-Suma(Transicion(E(z),E(x)), x <> z;

ELSE IF (hay diagnostico)
    FOR m -> 1 to k
        Transicion(E(0),E(k))= (1-beta)*lambda k;
        Transicion(E(k),E(0))= 1/MTTR;
    END FOR
    IF n>1
        FOR n -> 2 to j
            FOR m -> 1 to k
                Transicion(E(n-1),E(n,m))= lambda n,m;
            END FOR
        END FOR
        Transicion(E(j,k),E(0))= 1/(MTTR);
    END IF

    Transicion(E(0),E(D))=beta;
    Transicion(E(D),E(0))=1/(T2+MTTR);

    Transicion(E(z),E(z))=1-Suma (Transicio(E(z),E(x)), x <> z;
END IF
```

9.4. Aplicación de metodología para el análisis de arquitecturas mediante cadenas de Markov

Gracias a los modelos por cadenas de Markov, es posible representar todas las arquitecturas mediante estados de operación. Por ejemplo, si se tiene una arquitectura 2oo2 con dos unidades en paralelo, el sistema opera con las dos unidades funcionales; o con una unidad funcional y la otra en falla, donde además la unidad en falla se puede reparar mientras la segunda da soporte.

Arquitectura 1oo1: La cadena para la arquitectura 1oo1 está compuesta por cuatro estados, ver figura 28, donde cada estado representa la situación de los 3 elementos (1 entrada, 2 lógica y 3 salida). El primer estado se compone por los tres elementos funcionando de manera adecuada (OK). A los demás estados es posible llegar cuando se presente un fallo en alguno de los elementos del sistema, es decir, si se presenta una falla en un elemento se identifica en el estado con un fallo no detectado (FU) y es posible llegar a ellos con la tasa de fallos respectiva del elemento involucrado. Al ser un modelo reparable, el valor de μ (probabilidad de reparación) se expresa mediante $1/MTTR$ del elemento en el cual se presentó la falla. Sin embargo, como los fallos son no detectados, es necesario que se aplique el factor T2 de pruebas de diagnóstico al $MTTF$.

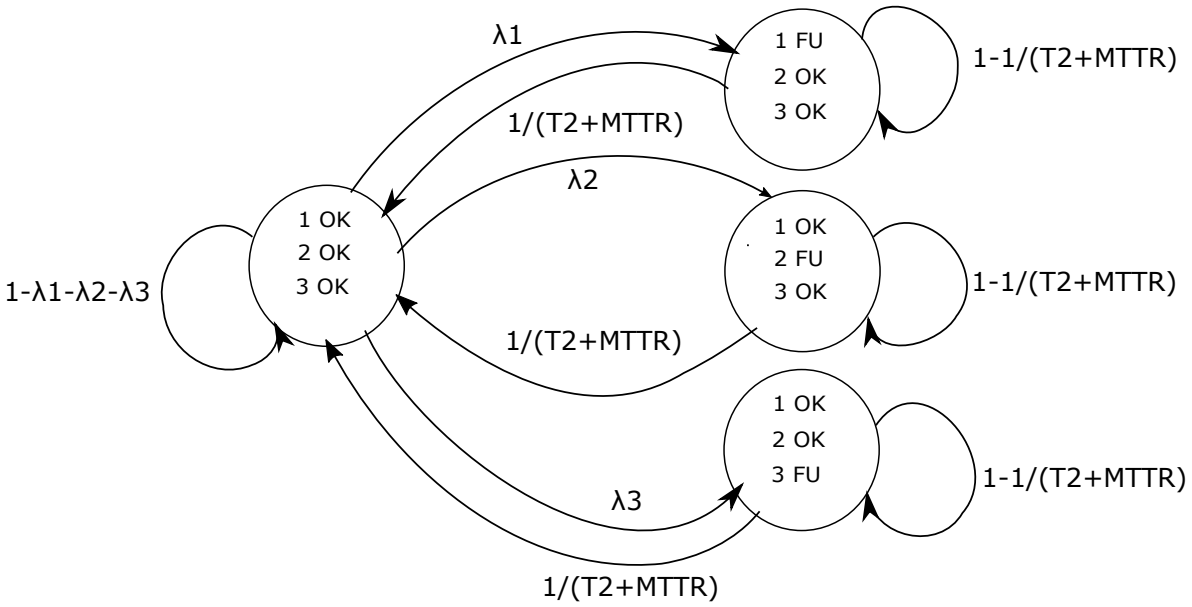


Figura 28. Análisis de transiciones arquitectura 1oo1. Fuente el autor.

Las transiciones que se pueden observar saliendo de un estado y entrando al mismo, expresan la probabilidad de permanencia del sistema en dicho estado.

El anterior modelo de Markov puede ser descrito mediante la siguiente matriz de transiciones, con la cual se puede modelar su funcionamiento.

$$\begin{bmatrix} 1-\lambda 1-\lambda 2-\lambda 3 & \lambda 1 & \lambda 2 & \lambda 3 \\ 1/(T2+MTTR) & 1-1/(T2+MTTR) & 0 & 0 \\ 1/(T2+MTTR) & 0 & 1-1/(T2+MTTR) & 0 \\ 1/(T2+MTTR) & 0 & 0 & 1-1/(T2+MTTR) \end{bmatrix}$$

Para hallar el *PFHd*, a partir de la matriz de transiciones, se encuentra el *MTBF* y luego se invierte para obtener el *PFHd*, tal como se mostró en la sección 8.1.

$$PFHd : \lambda_1 * (\frac{1}{T_2 + MTTR}) + \lambda_2 * (\frac{1}{T_2 + MTTR}) + \lambda_3 * (\frac{1}{T_2 + MTTR})$$

Arquitectura 1oo1D: La cadena para la arquitectura 1oo1D, ver figura 29, está compuesta por cinco estados, representando la situación en la cual se encuentran los tres elementos involucrados (1 entrada, 2 lógica y 3 salida). El primer estado se compone por los tres elementos funcionando de manera adecuada (OK). A los demás estados es posible llegar cuando se presente un fallo en alguno de los elementos del sistema. En esta cadena, al existir la capacidad de comprobación, los fallos que se presentan son fallos detectados, y por consiguiente no se hace necesaria la aplicación de las pruebas de diagnóstico. (1- β) es la probabilidad de que no se presente un fallo por causa común.

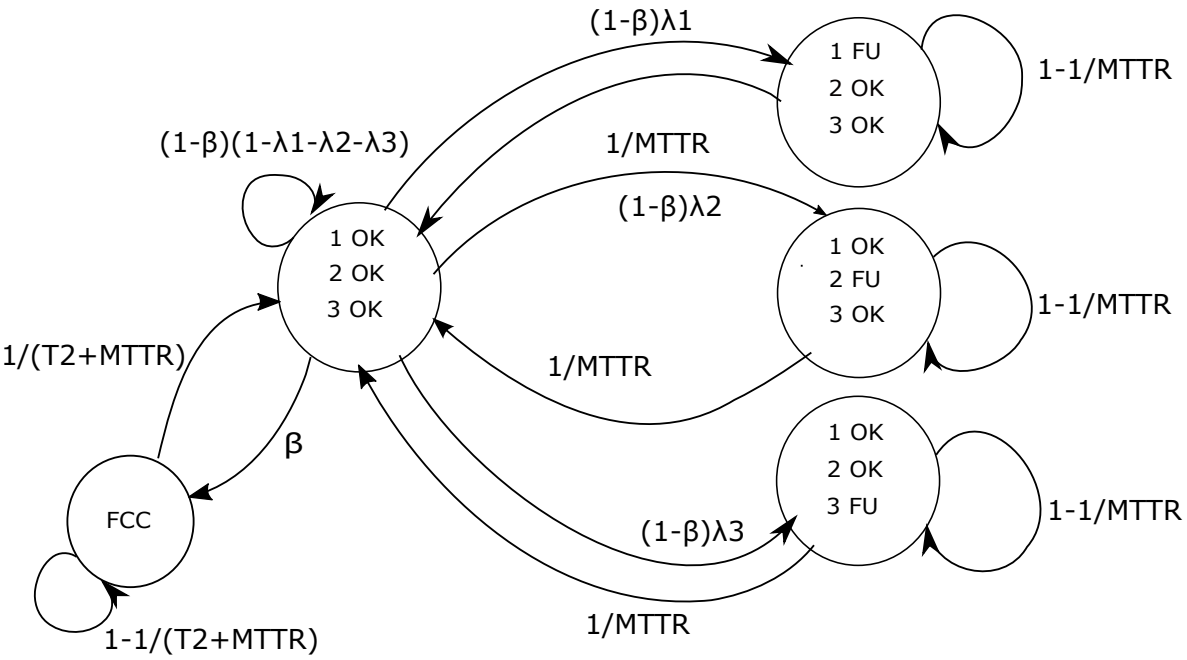


Figura 29. Diagrama Markov 1oo1D. Fuente el autor.

El anterior modelo de Markov puede ser descrito mediante la siguiente matriz de transiciones, con la cual se puede observar su funcionamiento.

$$\begin{bmatrix} (1-\beta)(1-\lambda 1-\lambda 2-\lambda 3) & (1-\beta)\lambda 1 & (1-\beta)\lambda 2 & (1-\beta)\lambda 3 & \beta \\ 1/MTTR & 1-1/MTTR & 0 & 0 & 0 \\ 1/MTTR & 0 & 1-1/MTTR & 0 & 0 \\ 1/MTTR & 0 & 0 & 1-1/MTTR & 0 \\ 1/(T2+MTTR) & 0 & 0 & 0 & 1-1/(T2+MTTR) \end{bmatrix}$$

Nuevamente, para hallar el *PFHd*, a partir de la matriz de transiciones, se procede como se indica en la sección 8.1.

$$PFHd : (1-\beta) * (\lambda_1 * (\frac{1}{MTTR}) + \lambda_2 * (\frac{1}{MTTR}) + \lambda_3 * (\frac{1}{MTTR})) + \beta * (\frac{1}{T_2 + MTTR})$$

Arquitectura 1oo2 y 2oo2: La cadena para las arquitecturas 1oo2 y 2oo2 está compuesta por 2 canales, lo cual lleva a 4 componentes a tener en cuenta operando simultáneamente (i-entradas, L1-lógica 1, L2-lógica 2 y O-salidas). La cadena en general consta de 11 estados (ver figura 30), de los cuales se pueden destacar 3 conjuntos, el primero es un estado de funcionamiento correcto del sistema, donde todos los elementos funcionan. El segundo grupo de estados está conformado por 4 estados que representan la falla de uno de los elementos, pero al existir dos canales el sistema conserva su función de seguridad, permitiendo que opere con normalidad. El tercer grupo de estados está conformado por 6 estados, en los cuales después de tenerse un fallo previo se presenta un segundo fallo, haciendo que automáticamente se pierda la función de seguridad, y obligando a que el sistema tenga que ser reparado en su totalidad para poder volver a funcionar, es decir, volver al estado inicial donde se tienen todos los elementos del sistema funcionando con normalidad.

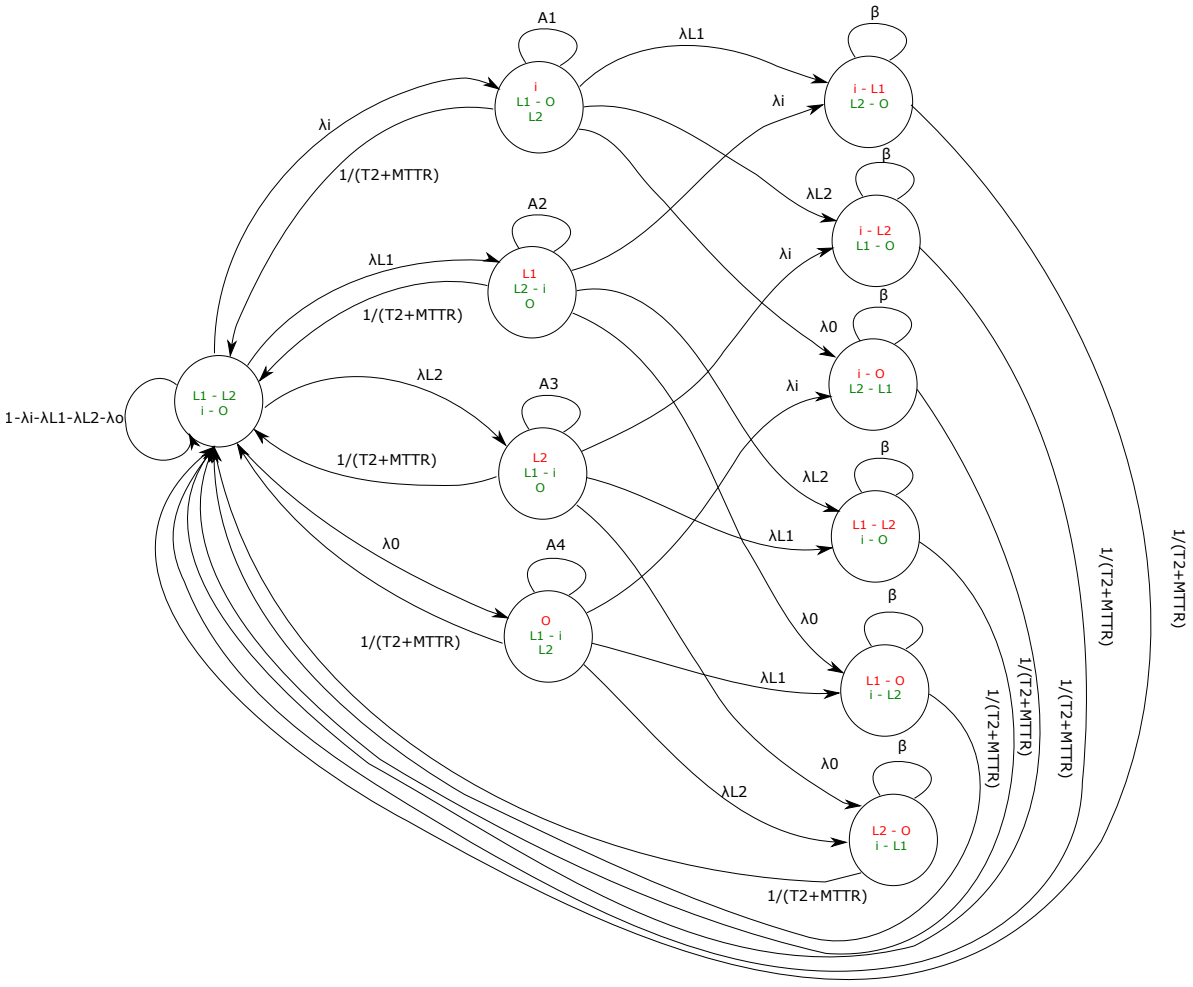


Figura 30. Diagrama Markov 1oo2 y 2oo2. Fuente el autor.

Para esta cadena es necesario tener en cuenta los datos que se muestran en la tabla 8, la cual indica los valores de las variables indicadas en la figura 30.

Símbolo	Equivalencia
A0	(1-λi-$\lambda L1$-$\lambda L2$-λ_0)
A1	1-(1/$T2$+$MTTR$)-$\lambda L1$-$\lambda L2$-λ_0
A2	1-(1/$T2$+$MTTR$)-λi-$\lambda L2$-λ_0
A3	1-(1/$T2$+$MTTR$)-λi-$\lambda L1$-λ_0
A4	1-(1/$T2$+$MTTR$)-λi-$\lambda L1$-$\lambda_L 2$
B	1-(1/$T2$+$MTTR$)

Tabla 8. Resumen de valores para arquitecturas 1oo2 y 2oo2.

Como se puede observar, mediante los colores rojos, las fallas son detectadas en todo el sistema; además, debido a que este tipo de arquitectura no cuenta con pruebas de diagnóstico es necesario tener en cuenta el factor $T2$.

La matriz de transiciones es la siguiente:

$$\begin{bmatrix}
A0 & \lambda i & \lambda L1 & \lambda L2 & \lambda 0 & 0 & 0 & 0 & 0 & 0 \\
0 & & & & & & & & & \\
1/T2 + MTTR & A1 & 0 & 0 & 0 & \lambda L1 & \lambda L2 & \lambda 0 & 0 & 0 \\
0 & & & & & & & & & \\
1/T2 + MTTR & 0 & A2 & 0 & 0 & \lambda i & 0 & 0 & \lambda L2 & \lambda 0 \\
0 & & & & & & & & & \\
1/T2 + MTTR & 0 & 0 & A3 & 0 & 0 & \lambda i & 0 & \lambda L1 & 0 \\
\lambda 0 & & & & & & & & & \\
1/T2 + MTTR & 0 & 0 & 0 & A4 & 0 & 0 & \lambda i & 0 & \lambda L1 \\
\lambda L2 & & & & & & & & & \\
1/T2 + MTTR & 0 & 0 & 0 & 0 & \beta & 0 & 0 & 0 & 0 \\
0 & & & & & & & & & \\
1/T2 + MTTR & 0 & 0 & 0 & 0 & 0 & \beta & 0 & 0 & 0 \\
0 & & & & & & & & & \\
1/T2 + MTTR & 0 & 0 & 0 & 0 & 0 & 0 & \beta & 0 & 0 \\
0 & & & & & & & & & \\
1/T2 + MTTR & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \beta & 0 \\
0 & & & & & & & & & \\
1/T2 + MTTR & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \beta \\
0 & & & & & & & & & \\
1/T2 + MTTR & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\beta & & & & & & & & &
\end{bmatrix}$$

Recurriendo a la sección 8.1, se puede hallar el *PFHd*, dando como resultado:

$$PFHd : (\lambda i) * (\frac{1}{MTTR + T2}) + \lambda_{L1} * (\frac{1}{MTTR + T2}) + \lambda_{L2} * (\frac{1}{MTTR + T2}) + \lambda_0 * (\frac{1}{MTTR + T2})$$

Arquitectura 1oo2D y 2oo2D: La cadena para las arquitecturas 1oo2D y 2oo2D está compuesta por 2 canales, lo cual lleva a 4 componentes a tener en cuenta operando simultáneamente (i-entradas, L1-lógica 1, L2-lógica 2 y O-salidas), tal como se observa en la figura 31. La cadena consta de 12 estados, de los cuales se pueden destacar 4 conjuntos: un estado de funcionamiento correcto del sistema, donde se tienen todos los elementos funcionando adecuadamente; un segundo conjunto compuesto por el estado

de falla por causa común, en el cual se presenta un fallo de todo el sistema de forma imprevista; un tercer conjunto conformado por 4 estados en los cuales se modelan las fallas en un único elemento, pero como existen dos canales, el sistema conserva su función de seguridad, permitiendo que opere con normalidad; y un cuarto grupo de estados conformado por 6 estados en los cuales después de existir un fallo, se presenta uno adicional, haciendo que automáticamente se pierda la función de seguridad, y obligando a que el sistema tenga que ser reparado para poder volver a funcionar, es decir, volver al estado inicial.

Es necesario tener en cuenta que para las primeras transiciones, es decir, entre el estado donde funciona todo adecuadamente y los estados donde se presenta un solo fallo, se debe aplicar el factor (1- β) que influye en la probabilidad de que se presente un fallo en un único elemento del sistema. Lo anterior asegura que en ese momento no se presente un fallo por causa común.

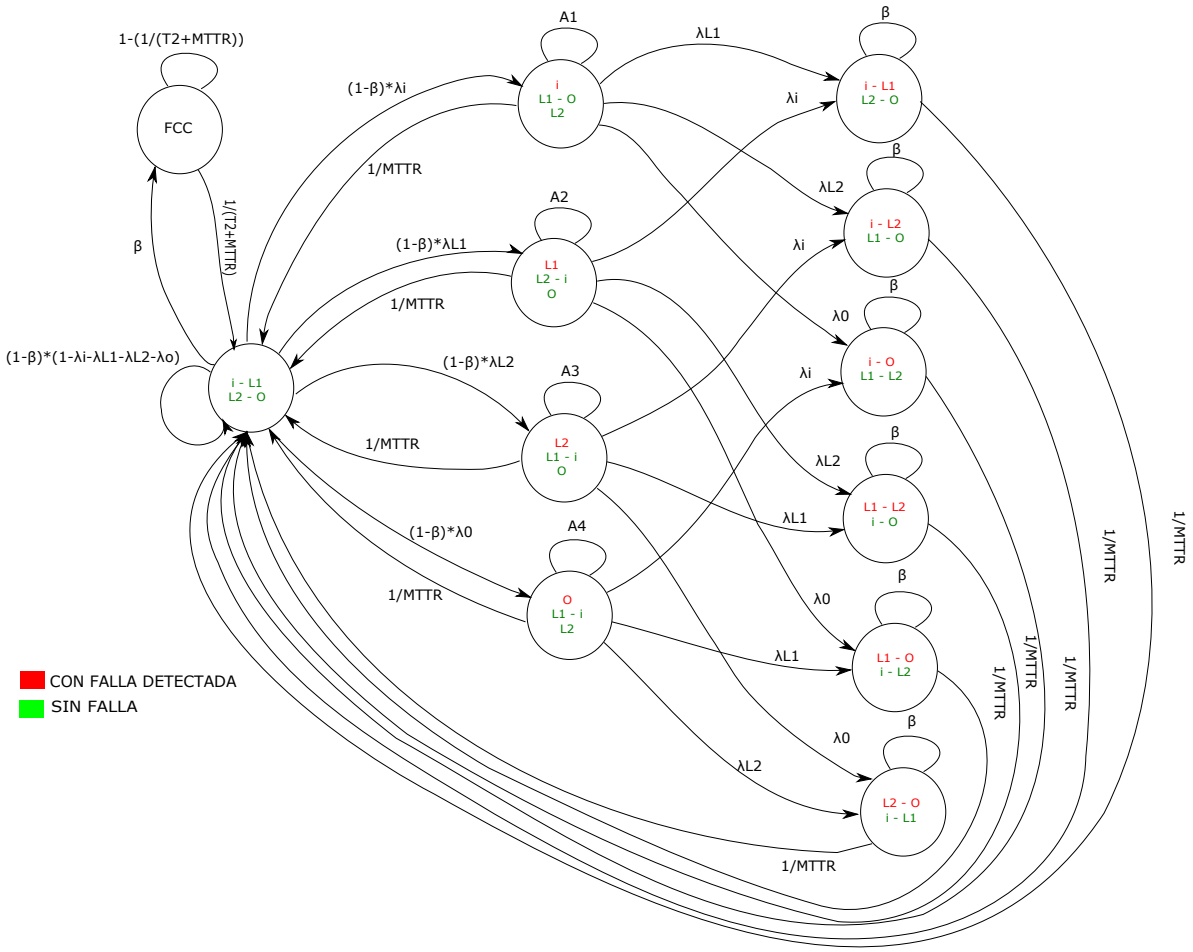


Figura 31. Máquina de estados 1oo2D y 2oo2D. Fuente el autor.

La tabla 9 presenta los valores de variables presentes en la figura 31.

Símbolo	Equivalencia
A0	(1-β)(1 − λi-$\lambda L1$-$\lambda L2$-λo)
A1	1-(1/$MTTR$)-$\lambda L1$-$\lambda L2$-λo
A2	1-(1/$MTTR$)-λi-$\lambda L2$-λo
A3	1-(1/$MTTR$)-λi-$\lambda L1$-λo
A4	1-(1/$MTTR$)-λi-$\lambda L1$-$\lambda L2$
B	1-(1/$MTTR$)

Tabla 9. Resumen de valores para arquitecturas 1oo2D y 2oo2D.

Como se puede observar, mediante los colores rojos, las fallas son detectadas en todo el sistema, con excepción de las fallas por causas comunes, las cuales siempre serán

no detectadas. Por ello, a la falla de causa común se le aplica el factor de pruebas de diagnóstico $T2$.

De lo anterior, la matriz de transiciones de Markov es la siguiente:

$$\begin{bmatrix}
A0 & (1-\beta)\lambda i & (1-\beta)\lambda L1 & (1-\beta)\lambda L2 & (1-\beta)\lambda 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \beta & & & & & & & & \\
1/MTTR & A1 & 0 & 0 & 0 & \lambda L1 & \lambda L2 & \lambda 0 & 0 & 0 \\
0 & 0 & & & & & & & & \\
1/MTTR & 0 & A2 & 0 & 0 & \lambda i & 0 & 0 & \lambda L2 & \lambda 0 \\
0 & 0 & & & & & & & & \\
1/MTTR & 0 & 0 & A3 & 0 & 0 & \lambda i & 0 & \lambda L1 & 0 \\
\lambda 0 & 0 & & & & & & & & \\
1/MTTR & 0 & 0 & 0 & A4 & 0 & 0 & \lambda i & 0 & \lambda L1 \\
\lambda L2 & 0 & & & & & & & & \\
1/MTTR & 0 & 0 & 0 & 0 & \beta & 0 & 0 & 0 & 0 \\
0 & 0 & & & & & & & & \\
1/MTTR & 0 & 0 & 0 & 0 & 0 & \beta & 0 & 0 & 0 \\
0 & 0 & & & & & & & & \\
1/MTTR & 0 & 0 & 0 & 0 & 0 & 0 & \beta & 0 & 0 \\
0 & 0 & & & & & & & & \\
1/MTTR & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \beta & 0 \\
0 & 0 & & & & & & & & \\
1/MTTR & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \beta \\
0 & 0 & & & & & & & & \\
1/MTTR & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\beta & 0 & & & & & & & & \\
1/MTTR & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1-1/(T2+MTTR) & & & & & & & &
\end{bmatrix}$$

De la sección 8.1, se puede hallar el *PFHd*, dando como resultado:

$$PFHd : (1-\beta) * (\lambda_i * (\frac{1}{MTTR}) + \lambda_{L1} * (\frac{1}{MTTR}) + \lambda_{L2} * (\frac{1}{MTTR}) + \lambda_o * (\frac{1}{MTTR})) + \beta * (\frac{1}{T2+MTTR})$$

9.5. Aplicación y validación de la metodología propuesta

9.5.1. Aplicación y validación de la metodología en un sistema de parada de emergencia

Como aplicación de la metodología expuesta, se muestra a continuación un sistema de detención o parada de emergencia para un motor trifásico, y el cual puede presentar una posible avería potencialmente peligrosa para los trabajadores y para el proceso en general. El sistema está diseñado con dispositivos de seguridad y consta de: dos pulsadores de parada (dispositivos de entrada), de los cuales uno servirá como respaldo del otro; dos PLC de seguridad (dispositivos de lógica) intercomunicados entre sí, los cuales controlan las entradas y las salidas del sistema; y por último dos contactores de seguridad (dispositivo de salida), los cuales se encargan de la desconexión total del motor, de este modo se tiene un respaldo en caso de que uno de los dos contactores no funcione. El esquema de funcionamiento de este tipo de parada de emergencia se presenta en la figura 32:

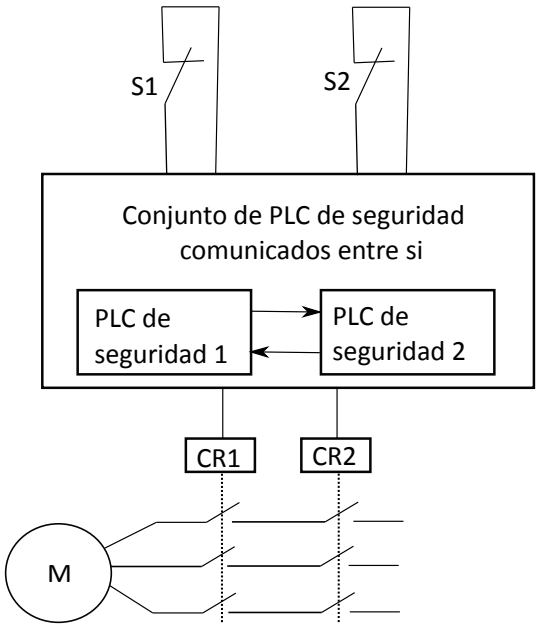


Figura 32. Funcion de seguridad ejemplo 1. Fuente el autor.

La presentación de la función de seguridad se muestra en la figura 33:

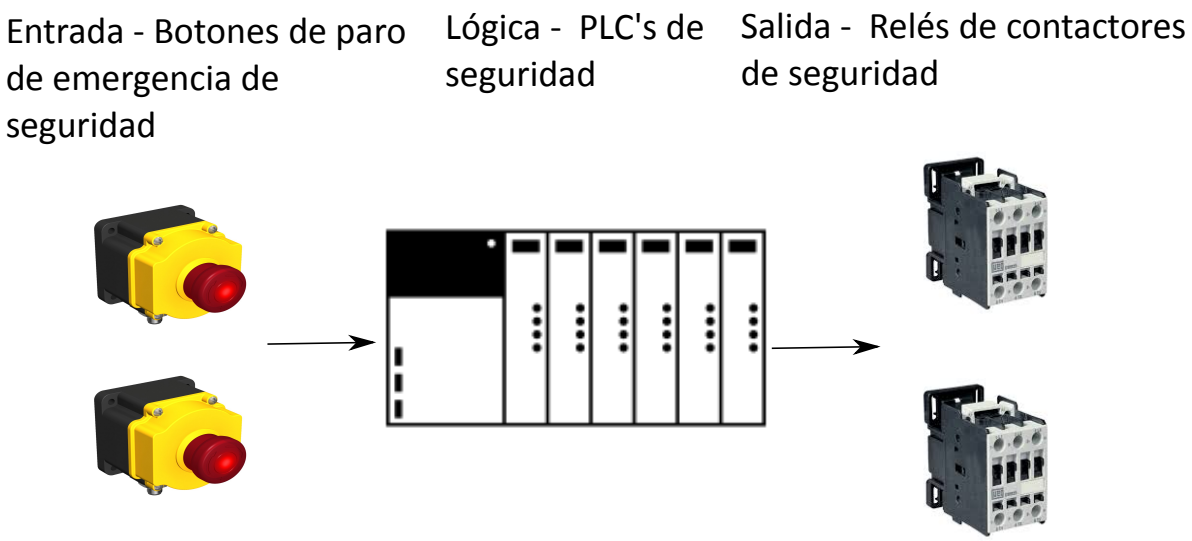


Figura 33. Representación de la funcion de seguridad para parada de emergencia. Fuente el autor.

Siguiendo los pasos de las normas IEC 61508 e IEC 61511, lo primero que se debe hacer es identificar el tipo de arquitectura con la cual se va a trabajar. Para este caso se tiene un sistema de dos canales, donde existen 2 entradas, 2 lógicas y 2 salidas y con dispositivos probados en seguridad, (ver figura 33). Por tanto, el sistema es una arquitectura 1oo2, para lo cual se debe utilizar el procedimiento expuesto para las arquitecturas 1oo2 y 2oo2.

A continuación, haciendo uso del árbol de selección, se debe calcular el *PLr* (ver figura 34). En este caso se tienen las siguientes condiciones:

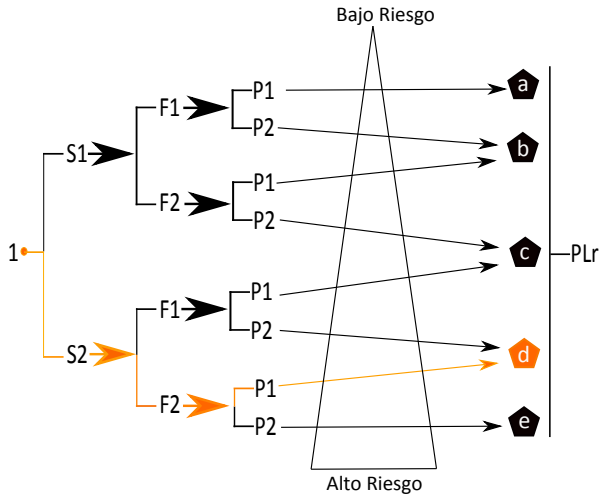


Figura 34. *PLr* de la funcion de seguridad ejemplo 1. Fuente el autor.

- **Importancia de los daños (S):** en el caso de una parada de emergencia de una máquina se tiene un nivel S2, donde se puede ocasionar una lesión grave (irreversible) y hasta la muerte en caso de que no se pueda detener.

- **Frecuencia y/o el tiempo de exposición que se tiene al peligro (F):** en este caso se tiene F2, debido a que se tiene una larga exposición y/o mayor frecuencia hasta permanente, por ser una máquina con uso diario.

- **Probabilidad de evitar el peligro o al menos minimizar los daños (P):** se toma como P1, ya que es posible evitar el riesgo en ciertas condiciones. De este modo se obtiene como resultado un *PLr*=d.

Continuando con los puntos siguientes del procedimiento por normas, se verifican los datos de reparación de este sistema, así que se tiene lo siguiente (se debe tener en cuenta que todos son dispositivos probados en seguridad):

***MTTR* de los pulsadores S1 y S2** = 32 horas.

***MTTR* de los PLC1 y PLC2** =160 horas.

***MTTR* de los relés de contactores CR1 y CR2** = 95 horas.

Valor $T2$ de intervalos de diagnóstico para FCC = 24 horas.

Luego se procede a revisar las hojas de datos de todos los elementos del sistema. Así, se pueden extraer los datos de las tasas de fallo de cada elemento:

λ **de los pulsadores S1 y S2** = 1,60x 10-4 fallas/hora

λ **de los PLC1 y PLC2** = 2,00x 10-5 fallas/hora

λ **de los relés de contactores CR1 y CR2** = 1.35x 10-4 fallas/hora

Ahora, para este tipo de arquitectura no es necesario identificar los fallos por causa común, sin embargo, si fuera necesario se utiliza el sistema de puntuaciones consignado en la tabla 1. Para este sistema se aplica lo siguiente:

Separación/Segregación = 15 puntos

Diversidad = 20 puntos

Diseño/Aplicación/Experiencia = 20 puntos

Competencia/Formación = 5 puntos Ambiental = 25 puntos

Otras influencias = 10 puntos

Con estas puntuaciones se tiene un total de 95 puntos, y consultando en la tabla 2, se tiene un factor de falla por causa común de:

$\beta = 0.1\,\%$ (es decir 0.001)

Ahora, se obtiene el valor del $PFHd$ según la arquitectura empleada (1oo2 en este caso) y haciendo uso de la cadena de Markov presentada en la figura 35:

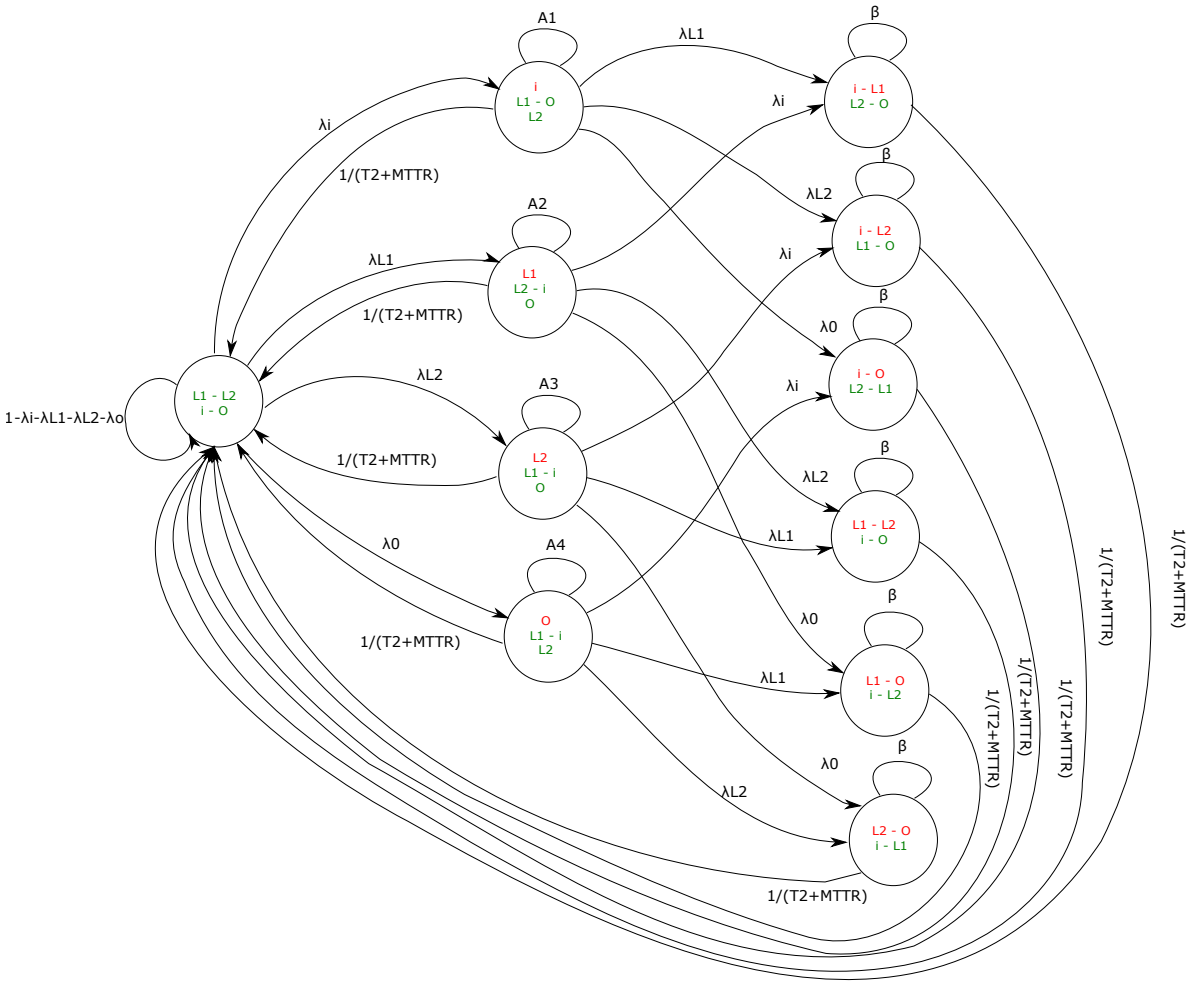


Figura 35. Cadena de Markov para parada de emergencia. Fuente el autor.

Al resolver la cadena de Markov de la arquitectura, se obtiene el valor del *PFHd* de todo el sistema.

$$PFHd : \lambda_i * (\frac{1}{MTTR + T2}) + \lambda_{L1} * (\frac{1}{MTTR + T2}) + \lambda_{L2} * (\frac{1}{MTTR + T2}) + \lambda_o * (\frac{1}{MTTR + T2})$$

Reemplazando valores, se logra:

$$PFHd : 2.8974 * 10^{-}6$$

Recordando que $MTTFd = 1/PFHd$, se puede obtener el valor del $MTTFd$ para todo el sistema, y además se debe pasar el valor a años, para poder identificar en donde se encuentra categorizado dicho término.

$$MTTFd : 345137.0194 = 39.4 \textbf{ años}$$

En la figura 36, se muestra gráficamente el valor del PL de todo el sistema.

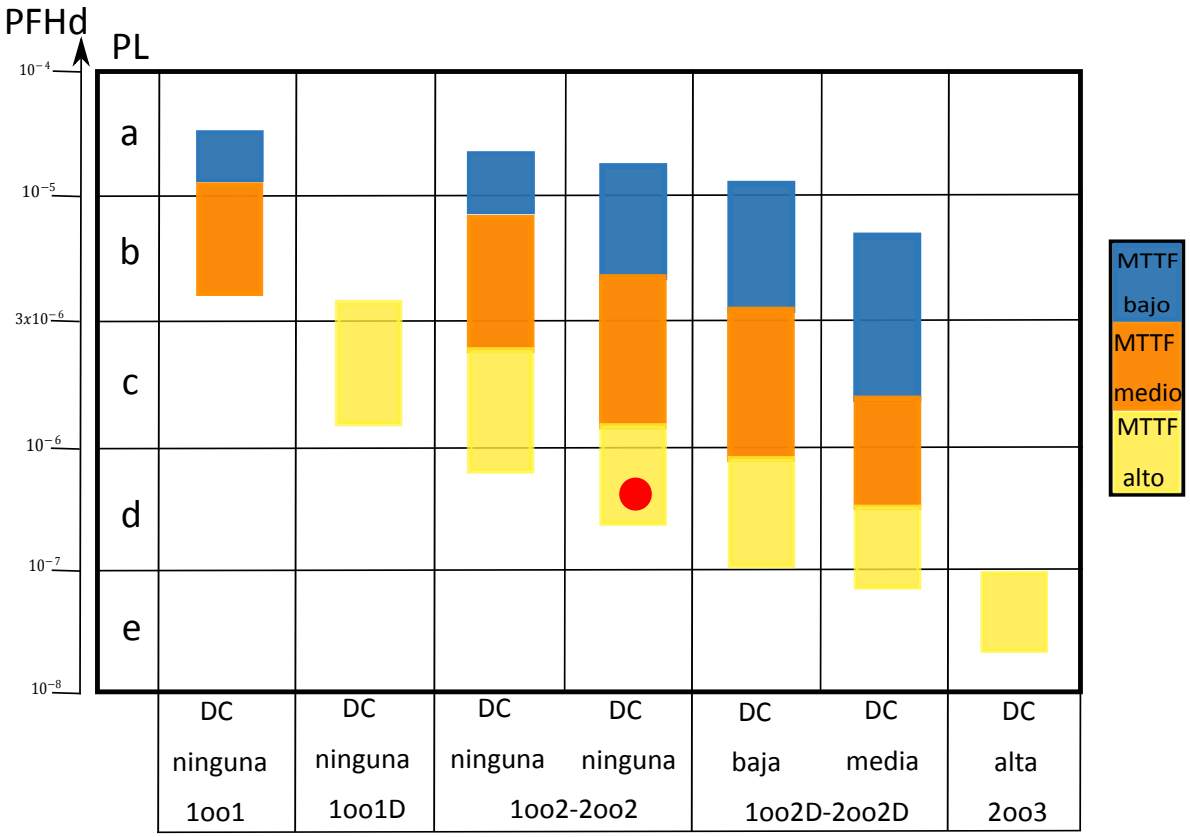


Figura 36. PL de la función de seguridad de parada de emergencia. Fuente el autor.

Con los parámetros calculados anteriormente, es posible obtener el PL del sistema. En la figura 36, el punto rojo representa el lugar donde se encuentran todos los parámetros hallados con anterioridad, y desde lo cual se puede concluir que se tiene un valor de PL=d. Por último, es necesario realizar la verificación de los PL:

$$PL \geq PLr$$

$$d \geq d$$

Con este resultado, se puede decir que el sistema está protegido bajo una categoría de $PL{=}d$, la cual es la que se necesita para este tipo de sistemas de paro de emergencia. Con esto se puede proceder a solicitar la validación de la función de seguridad (certificación), la cual debe ser realizada por personas diferentes a los encargados del diseño de dicha función de seguridad (para una revisión imparcial).

9.5.2. Aplicación y validación de la metodología en un sistema de enclavamiento de resguardo

Como segunda aplicación de la metodología propuesta, se muestra a continuación un sistema de enclavamiento de resguardo, el cual puede presentar una posible avería potencialmente peligrosa para los trabajadores y para el proceso en general. El sistema está diseñado con dispositivos de seguridad, los cuales deben detener el actuador cuando se abre el resguardo de seguridad.

Lo primero que se debe hacer es identificar el tipo de arquitectura. Para este caso, se tiene un sistema de un canal en el cual se tienen 1 entrada, 1 lógica y 1 salida y con dispositivos probados en seguridad. El sistema es de arquitectura 1oo1D.

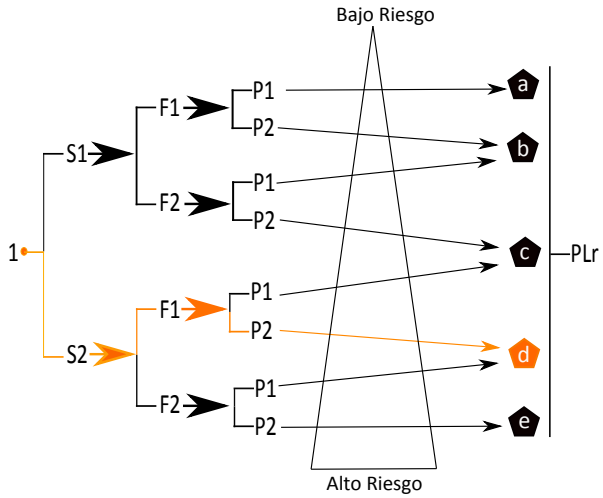


Figura 37. *PLr* de la función de seguridad para enclavamiento de resguardo. Fuente el autor.

Para calcular el *PLr* se utiliza el árbol de selección indicado en la figura 37. En este caso se tienen las siguientes condiciones:

- **Importancia de los daños (S):** se tiene un nivel S2, donde se puede ocasionar una lesión grave (irreversible).

- **Frecuencia y/o el tiempo de exposición que se tiene al peligro (F):** en este caso se tiene F1, debido a que se tiene una corta exposición y/o poca frecuencia a fuente de peligro.

- **Probabilidad de evitar el peligro o al menos minimizar los daños (P):** se toma como P2, ya que no es posible evitar el riesgo en ciertas condiciones.

De este modo se obtiene como resultado *PLr*=d.

Se prosigue con verificar los datos de reparación de este sistema, así que se tiene lo siguiente (se debe tener en cuenta que todos son dispositivos probados en seguridad):

***MTTR* S1**= 24 horas.

***MTTR* PLC** =70 horas.

***MTTR* relé de contactor CR** = 40 horas.

***MTTR* de los fallos por causa común** = 400 horas.

Valor T2 de intervalos de diagnóstico para FCC = 12 horas.

Luego, se debe obtener los datos de tasas de fallo de cada elemento, siendo los siguientes:

λ **S1** = 1,60x 10-5 fallas/hora

λ **PLC** = 2,00x 10-6 fallas/hora

λ **de relé contactor CR** = 1.35x 10-5 fallas/hora

Ahora, para este tipo de arquitectura es necesario identificar los fallos por causa común que puede tener este sistema. Para ello se utiliza la tabla 1, en la cual se encuentra el sistema de puntuaciones. Para este sistema aplica lo siguiente:

Separación/Segregación = 14 puntos

Diversidad = 18 puntos

Diseño/Aplicación/Experiencia = 20 puntos

Competencia/Formación = 4 puntos

Ambiental = 25 puntos

Otras influencias = 10 puntos

Con estas puntuaciones se tiene un total de 91 puntos, para lo cual se tiene un factor de falla por causa común de:

$\beta = 0.1\,\%$ (es decir 0.001)

Luego, se procede a obtener el valor de la cobertura de diagnóstico, para lo cual se utilizan las tablas 3, 4, 5 y 6. Esta tablas ilustran la cobertura de diagnóstico, con sus respectivas condiciones. En este caso, los resultados de la cobertura de diagnóstico son:

99 % en la entrada.

90 % en la lógica.

90 % en la salida.

De estos tres datos, se elige el menor, ya que es con el que se tiene el peor caso, es decir, según la tabla 3, se tendrá una cobertura de diagnóstico igual a: 90 % $\leq$ DC $<$ 99 % Cobertura de diagnóstico Media.

Ahora, se debe verificar el valor del *PFHd*, que se puede obtener desde la cadena de Markov para una arquitectura 1oo1D, como se muestra en la figura 38:

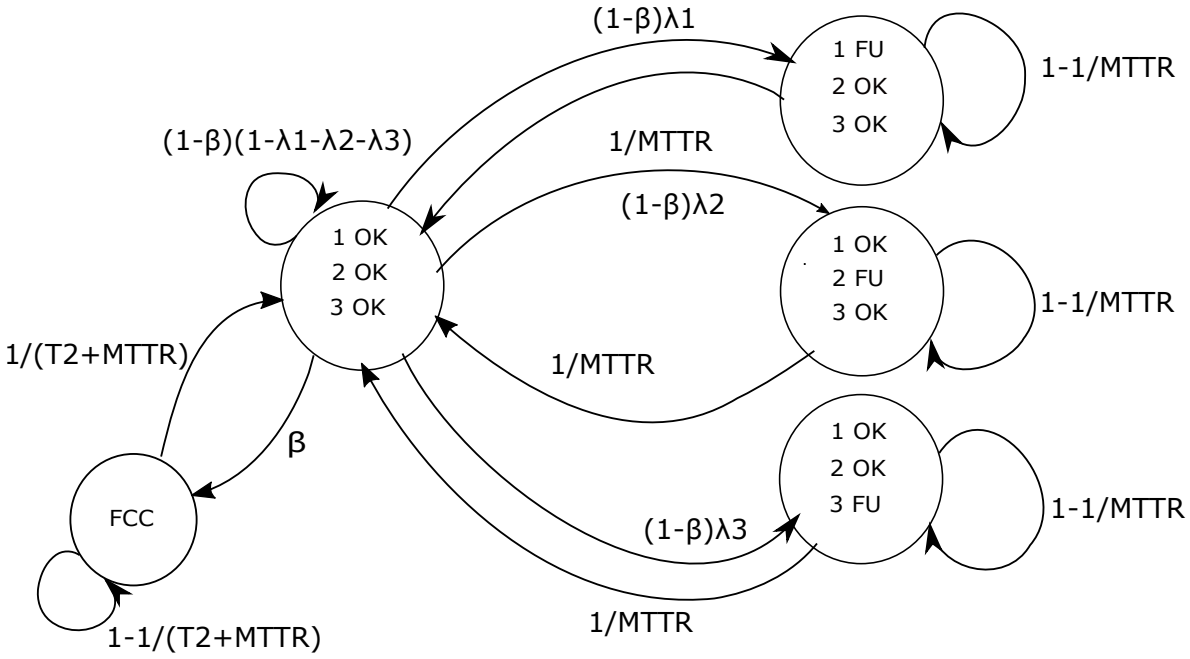


Figura 38. Cadena de Markov para enclavamiento de resguardo. Fuente el autor.

De la cadena de Markov anterior, se obtiene la siguiente solución, producto de reemplazaro los datos previos.

$$PFHd : (1-\beta) * (\lambda_1 * (\frac{1}{MTTR}) + \lambda_2 * (\frac{1}{MTTR}) + \lambda_3 * (\frac{1}{MTTR})) + \beta * (\frac{1}{MTTR})$$

$$PFH_d : 3.4589 * 10^{-6}$$

Recordando que $MTTFd = 1/PFHd$, se puede obtener el valor del $MTTFd$ para todo el sistema.

$$MTTFd : 289109,2544 = 33 \textbf{ años}$$

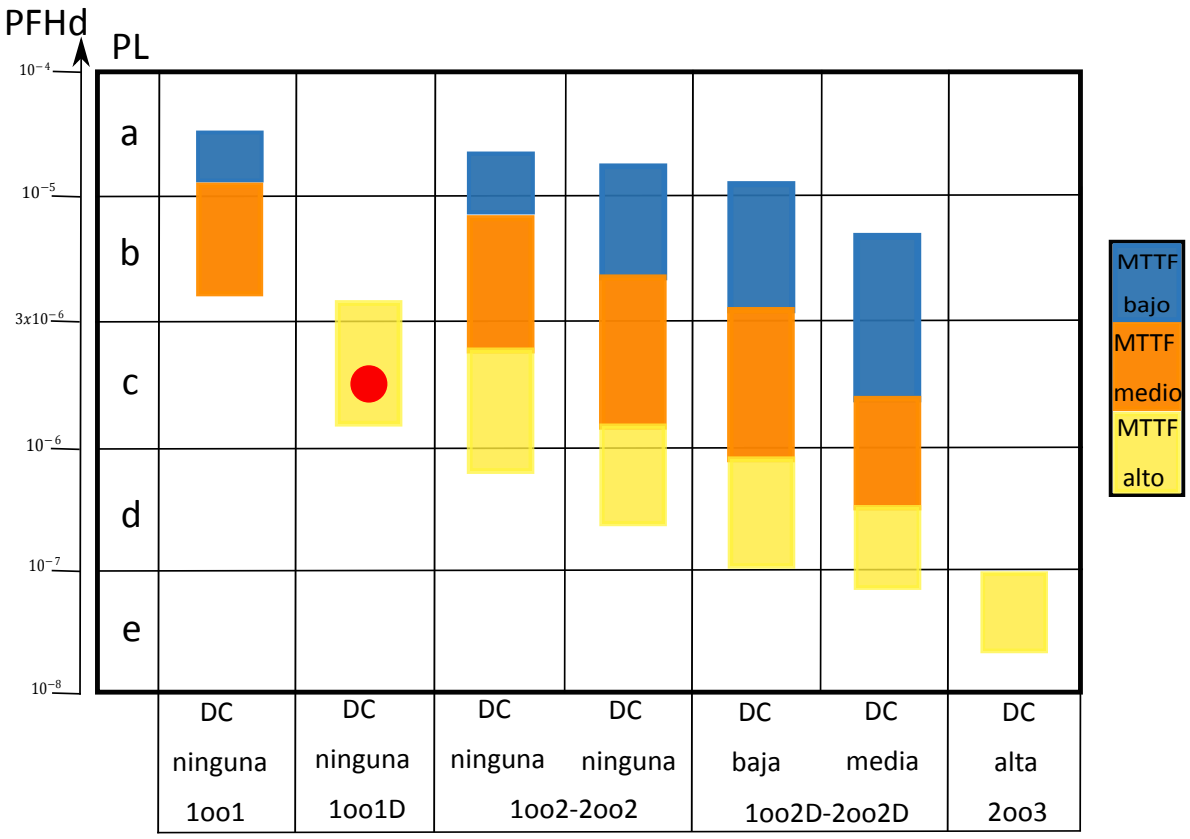


Figura 39. PLr del enclavamiento de resguardo. Fuente el autor.

Con los parámetros calculados anteriormente, se obtiene el PL del sistema. En la figura 39, el punto rojo representa el lugar donde se encuentran todos los parámetros hallados con anterioridad, y desde el cual se puede concluir que se tiene un valor de PL=c. Por último, es necesario realizar la verificación del PL:

$$PL \geq PLr$$

$$c \ngeq d$$

Con este resultado se puede decir que el sistema no está protegido bajo una categoría de PL=c, la cual es menor a la categoría de PL que se necesita para este tipo de sistemas de enclavamiento de resguardo. Por tal motivo, es necesario utilizar otro tipo de arquitectura ya que con la arquitectura implementada no es posible obtener un nivel de PL mayor.

De acuerdo al procedimiento sugerido por norma, entonces se procede a rediseñar el sistema buscando que el valor de PL determinado sea igual o superior al requerido. Por ello, se toma la arquitectura 1oo2 y se obtiene un

$$PFH_d : 7.52858 * 10^{-7}$$

, con el cual no es posible obtener un nivel PL. Por tal motivo, se hace necesario tomar componentes con mejores tasas de reparación y recalcular con base en una arquitectura 1oo2:

λ **S1** = 1,60x 10-4 fallas/hora

λ **de los PLC1 y PLC2** = 2,00x 10-5 fallas/hora

λ **de los relés de contactores CR1 y CR2** = 1.35x 10-4 fallas/hora.

Los tiempos de reparación permanecen iguales, así:

***MTTR* S1 y S2**= 24 horas.

***MTTR* de los PLC1 y PLC2** =70 horas.

***MTTR* relés de contactores CR1 y CR2** = 40 horas.

Valor T2 de intervalos de diagnóstico para FCC = 12 horas.

Al utilizar la ecuación del PFHd para la arquitectura 1oo2 se obtiene:

$$PFH_d : 7.5239 * 10^{-6}$$

Como se muestra en la figura 40, al ubicar el valor hallado, se determina que el nuevo valor corresponde a la categoría d.

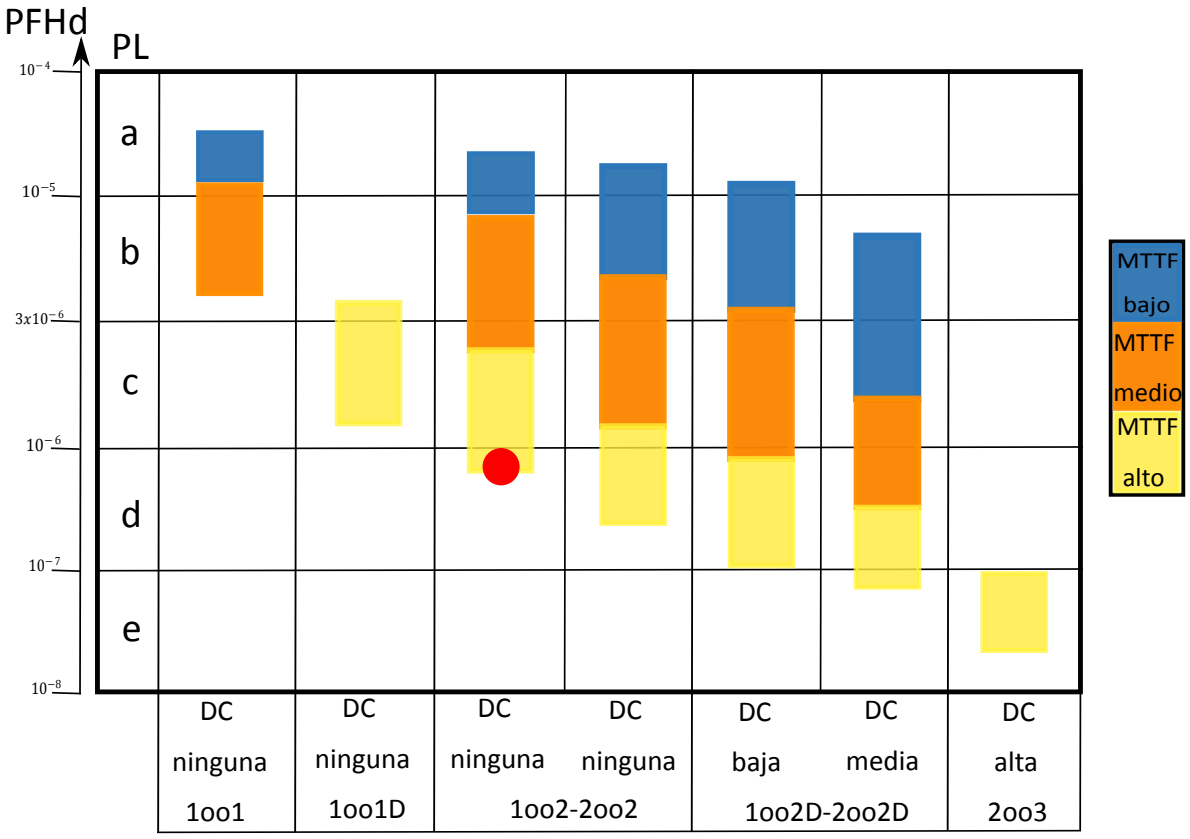


Figura 40. *PLr* del enclavamiento de resguardo rediseñado en arquitectura 1oo2. Fuente el autor.

Verificando,

$$PL \geq PLr$$

$$d \geq d$$

Con este último resultado, el sistema esta protegido con una categoría PL=d, la cual es la requerida para este sistema de enclavamiento de resguardo.

9.6. Conclusiones

- Los requerimientos contenidos en las normas IEC 61508 e IEC 61511 demandan la implementación del ciclo de vida de la seguridad, para lo cual definen los procedimientos generales para el diseño y/o análisis de sistemas de seguridad para la industria moderna, mediante la identificación y reducción de los riesgos asociados. Esto se logra mediante sistemas integrados de seguridad que implementan funciones instrumentadas de seguridad diseñadas para lograr niveles de prestación requeridos y adecuados al riesgo inherente.

- Con el fin de cumplir con el nivel de prestación requerido, se presenta una serie de arquitecturas que permiten implementar las funciones instrumentadas de seguridad, que adicionando niveles de redundancia y comprobación mediante el uso de uno o varios canales de implementación, o el uso de vías de diagnóstico, permiten mejorar los requerimientos esperados en cuanto al tiempo medio entre fallas $MTTF$.

- Para determinar el nivel de prestación de una arquitectura y sistema específico, en este documento se explora y presenta una metodología basadas en el uso de cadenas de Markov con el fin de analizar y obtener el valor del $MTTF$. La metodología presentada muestra su poder de adaptación a todas las arquitecturas existentes e incluso su poder de extensión a cualquier modificación o ajuste requerido. La metodología permite describir sistemas con diferentes números de canales de operación, con la presencia de elementos en redundancia y con la posibilidad de incluir cobertura para el diagnóstico.

- La metodología presentada se aplica y valida en dos sistemas comunes presentes en la industria. En estas aplicaciones, se evidencia su adaptación para permitir diseñar y analizar los niveles de prestación para un sistema, y su comprobación respecto al nivel de prestación requerido y/o demandado.

- Finalmente, se puede concluir que se ha desarrollado una metodología que se adapta para permitir cumplir las demandas en seguridad que se presentan en plataformas industriales desactualizadas, empleando el ciclo de vida de la seguridad, así como funciones y sistemas instrumentados de seguridad, de acuerdo con las normativas IEC 61508 y 61511, y aplicando las cadenas de Markov como medio para describir y analizar los nuevos requerimientos en seguridad.

9.7. Trabajos derivados

Como parte del desarrollo del presente proyecto de grado se presentó a consideración, y fue aprobada y presentada, la siguiente ponencia en evento internacional:

- Metodología para la aplicación de sistemas de seguridad en procesos industriales. III Congreso Internacional de Electromecánica y Eléctrica; 2, 3 y 4 de septiembre de 2020, Ecuador. Carlos Ariel García Montoya, Sebastián Aguirre Vargas, Mauricio Holguín Londoño.

9.8. Trabajos futuros

- Se propone ahondar en la exactitud del modelado por cadenas de Markov en cuanto a la necesidad de incluir, o excluir, estados en la representación de un sistema. Este aspecto es importante, toda vez que a mayor cantidad de estados

mejor representación del sistema, pero mayor carga computacional para la solución de la matriz de Markov asociada.

- Las arquitecturas presentadas y los respectivos modelos de Markov asociados, parten del hecho de poder tener múltiples canales asociados a la lógica o a la conexión/desconexión de la salida. Pero estos modelos no exploran la incorporación de redundancia en las entradas o en los actuadores finales. Estas posibilidades abren todo un campo de estudio a ser tenido presente en futuros desarrollos.

BIBLIOGRAFÍA

[1] J. RIVAS ESCUDERO Y P. M. REDONDO SOBRADO. SISTEMAS INSTRUMENTADOS DE SEGURIDAD (SIS):CICLO DE VIDA, 2007. (document), 1, 4.2, 1

[2] J. BIELZA. PLCdesign Sistemas de control, 26 Mayo 2016. URL http://plcdesign.xyz/que-es-un-plc-de-seguridad/. Último acceso: 30 05 2020. (document), 2

[3] K. RÁSTOCNý, J. ILAVSKý. Quantification of the safety level of a safety-critical control system, 2010. 1

[4] K. RASTONCY, P. NAGY. Operator's Influence on the Safety of the Controlled Process, 2015. Vol 13 n°3. 1

[5] SMART. SIS Sistema Instrumentado de Seguridad. URL http://www.smar.com/espanol/articulos-tecnicos/sis-sistemas-instrumentados-de-seguridad. Último acceso: 20 ENERO 2020. 1

[6] L. G. PECSÉN. SISTEMAS INSTRUMENTADOS DE SEGURIDAD (SIS). GN - La Revista del Gas Natural. 1

[7] SCHNEIDER ELECTRIC. Seguridad de personas y máquinas cap 7 pag 160 a 182,. URL https://es.rs-online.com/es/pdf/Schneider.pdf. Último acceso: 15 Marzo 2020. 1, 2

[8] E. S. TORRES, S. SRIRAMULA, D. CELEITA Y G. RAMOS. Model for Assessing the Safety Integrity Level of Electrical/ Electronic/Programmable Electronic Safety-Related Systems, 2019. 1, 2, 4.3

[9] R. E. COSSÉ, H. T. COMBS, M. A. HILDRETH, J. E. BOWEN, D. G. DUNN Y A. PILCHER. Smart industrial substations-a modern integrated approach, 2003. 2

[10] T. ESPERANZA S, S. SRIRAMULA, D. CELEITA, G. RAMOS. Reliability Model and Sensitivity Analysis for Electrical/ Electronic/Programmable Electronic Safety-Related Systems, 2019. 2, 4.1, 4.3, 4.4

[11] CANALES SECTORIALES INTEREMPRESAS-GREG COOKE. Aumento de la rentabilidad mediante la actualizacion y sustitucion de los equipos, Julio 2010. URL https://www.interempresas.net/Plastico/Articulos/36716-Aumento-de-la-rentabilidad-mediante-la-actualizacion-y/-sustitucion-de-los-equipos.html. Último acceso: 15 Marzo 2020. 2

[12] J. BÖRCSÖK. Safety Systems, Germany, 2004. HIMA Paul Hildebrandt GmbH + Co KG. 2, 4.1

[13] J. CASTELLANOS. Validación del SIL de un proceso, 2004. Invensys Systems Ibérica, nº Julio/ Agosto, pp. 149-154. 2

[14] IEC 61508. Functional safety of electrical/electronic/programmable electronic safety-related systems, parts 1-7, 2010. Geneva, Switzerland: International Electrotechnical Commission. 2, 4.1

[15] IEC 61511. Funtional safety: safety instrumented systems for the process industry sector, parts 1-3, 2016. Parts 1-3, Geneva, Switzerland: International Electrotechnical Commission. 2, 4.1

[16] ISA-TR84.00.02. Safety Integrity Level (SIL) verification of safety instrumented functions, 2015. International Society of Automation, Nort Carolina; US, 2015. 2, 4.1

[17] J. BÖRCSÖK. Functional Safety: Basic Principles of Safety-related Systems, 2007. Heidelberg, Germany: Hüthig GmbH Co. KG, 2007. 4.1

[18] E. P. MANAGEMENT. Normas de seguridad, 2005. URL https://www.emerson.com/documents/automation/training-sis-103-safety-standards-es-es-41618.pdf. Último acceso: 15 Junio 2020. 4.1

[19] L. GALÁN. Normativa IEC para la seguridad, 1 julio 2009. URL http://www.emb.cl/electroindustria/articulo.mvc?xid=1224. 20 febrero 2020. 4.1

[20] E. H. DOGRUGUVEN, I. USTOGLU. An Evaluation of Safety Standards of E/E/PES System Regarding Information Consistency Enhancement Proposals, 2019. IEEE. 4.1

[21] N. PAPAKONSTANTINOU, S. SIERLA, J. ALANEN, K. KOSKINEN. Reducing Redesign of Safety Critical Control, 2010. IEEE, pp. 460-465. 4.1

[22] GOOGLE.COM. URL https://www.google.com/search?q=sil+(security+integrity+level)+-+nivel+de+integridad+de+la+seguridad&source=lnms&tbm=isch&sa=X&ved=0ahUKEwj13cPFz-rlAhURRa0KHezPAxoQ_AUIEigB&biw=1366&bih=646#imgrc=cSqerZU_5rKdCM. Último acceso: 20 Enero 2020. 4.4

[23] Z. DU, G. CHENG, M. WANG, R. SUN Y K. LIU. Research on Safety Programmable Controller Based on Dual-CPU Architecture, 2019. IEEE, pp. 2034-2038. 4.5, 4.5

[24] J. ZDANSKY Y P. NAGY. Influence of the Control System Structure with Safety PLC on its Reliability and Safety, 2012. IEEE, pp. 395-399. 4.5

[25] O. ODARUSHCHENKO, O. STRJUK, Y. BULBA, K. LEONTIIEV, A. IVASYUK, V. KHARCHENKO. Fault Insertion Software and Hardware Testing for Safety PLC-Based System SIL Certification, 2018. IEEE, vol. The 9th IEEE International Conference on Dependable Systems, pp. 202-206. 4.5

[26] REVISTA INTECH MÉXICO AUTOMATIZACIÓN, 2007. URL https://pdfslide.net/documents/arquitecturas-de-votacion.html. InTech, Vols. 1 de 2 Octubre- Diciembre, p. 138 a 143, 2007. 4.5

[27] J. HOLMES. Safety integrity level requirements in deepwater drilling — Where safety meets reliability, 2015. 2015 Annual Reliability and Maintainability Symposium (RAMS), Palm Harbor, FL. 5, 5.1, 5.2

[28] A. R. ARANGO. Metodología implementación de algoritmos tolerables a fallos para automatismos industriales bajo el estándar IEC 61508, 2012. Universidad Tecnológica de Pereira, 2012. 5.1, 5.2, 5.2

[29] N. D. RIOS GONZALES Y J. O. SALAZAR SALDARRIAGA. Metodología basada en cadenas de Markov para evaluar niveles de seguridad en sistemas de mando según las normas EN ISO 13849-1 y EN IEC 62061-1, 2012. Universidad tecnológica de Pereira, 2012. 5.1, 5.3, 5.3, 5.3, 6.4, 7, 7, 7, 7, 7, 7, 7

[30] J. ŽDÁNSKY, K. RÁSTOčNý AND J. HRBčEK. Influence of architecture and diagnostic to the safety integrity of SRECS output part, 2015. 2015 International Conference on Applied Electronics (AE), Pilsen,. 5.1, 5.2

[31] J. B. ALDARONDO Y I. U. ESTÉBANEZ. Diseño de las partes de los sistemas de mando relativas a la seguridad, 2012. Instituto Nacional de Seguridad e Higiene en el Trabajo, 2012. 5.3

[32] J. VALIGURSKý. Influence of SRCS architecture on possibility to achieve required safety integrity level of safety function, 2020. 2020 Cybernetics Informatics (KI), Velke Karlovice, Czech Republic, 2020. 6.2

[33] J. J. SAMMARCO. Programmable Electronic and Hardwired Emergency Shutdown Systems: A Quantified Safety Analysis, 2017. In IEEE Transactions on Industry Applications, vol. 43, no. 4, July-aug. 2007. 6.3

[34] J. JIN, W. XIONG AND P. XU. Research on Architectural Constraints Analysis and an Improvement Method for Safety Instrumented Systems, 2018. 2018 12th International Conference on Reliability, Maintainability, and Safety (ICRMS), Shanghai, China, 2018. 7, 7

[35] M. H. LONDOÑO. Filosofías de Mantenimiento: Modelo predictivo – Cadenas de Markov, 2020. Universidad Tecnológica de Pereira, 2020. 8.1, 8.1, 8.1, 8.1, 8.2

[36] J. V. BUKOWSKI. A unified model for evaluating the safety integrity level of safety instrumented systems, 2012. 2008 Annual Reliability and Maintainability Symposium, Las Vegas, NV, 2008. 8.1